



WEB APPLICATION FIREWALL

FortiWeb™ 5.3

Log Reference



FortiWeb 5.3 Log Reference

September 15, 2014

1st Edition

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard® and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	http://help.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forum
Customer Service & Support	https://support.fortinet.com
Training	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
License	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: techdocs@fortinet.com

Table of contents

Introduction.....	12
Scope.....	12
What's new.....	13
How to interpret FortiWeb logs.....	15
Header & body fields	15
Log ID numbers	23
Types	23
Subtypes.....	24
Priority level	24
Message IDs	25
Event.....	26
Reboot, shut down, & boot up messages	38
00001002	39
00001012	40
00001052	41
00001062	42
00002202	43
00002801	44
00002802	45
00002811	46
00003401	47
00003402	48
00003411	49
00004401	50
00004402	51
00004411	53
00004902	54
00006001	55
00006002	56
00006011	57
00006102	58
00006202	59
00006302	60
00006501	61
00006502	62

00006511	63
00007302	64
00007402	65
00008101	66
00008102	67
00008111	68
00008602	69
00008701	70
00008702	71
00008711	72
00008801	73
00008811	74
00008901	75
00008911	76
00009001	77
00009011	78
00009101	79
00009111	80
00009201	81
00009211	82
00009301	83
00009311	84
00009401	85
00009402	86
00009411	87
00009501	88
00009502	89
00009511	90
00009702	91
00010001	92
00010002	93
00010011	94
00010201	95
00010202	96
00010211	97
00010401	98
00010402	99
00010411	100
00010501	101
00010502	102

00010511	103
00010601	104
00010602	105
00010611	106
00010701	107
00010711	108
00020088	109
00020201	110
00020202	111
00020211	112
00020301	113
00020302	114
00020311	115
00020801	116
00020802	117
00020811	118
00020901	119
00020902	120
00020911	121
00021002	122
00021102	123
00021140	124
00021202	125
00021302	126
00021402	127
00022997	128
00030001	129
00030002	130
00030011	131
00032006	132
00040001	133
00040002	134
00040011	135
00040301	136
00040302	137
00040311	138
00040501	139
00040502	140
00040511	141
00040601	142

00040611	143
00040623	144
00040751	145
00040752	146
00040761	147
00040801	148
00040802	149
00040811	150
00040901	151
00040902	152
00040911	153
00041001	154
00041002	155
00041011	156
00041101	157
00041102	158
00041111	159
00041201	160
00041202	161
00041211	162
00041302	163
00041401	164
00041402	165
00041411	166
00041601	167
00041602	168
00041611	169
00041801	170
00041802	171
00041811	172
00043001	173
00043002	174
00043011	175
00044001	176
00044002	177
00044011	178
00044401	179
00044411	180
00044501	181
00044502	182

00044511	183
00046001	184
00046002	185
00046011	186
00050001	187
00050002	188
00050011	189
00050201	190
00050202	191
00050211	192
00050401	193
00050402	194
00050411	195
00051001	196
00051002	197
00051011	198
00051201	199
00051202	200
00051211	201
00051401	202
00051402	203
00051411	204
00051601	205
00051602	206
00051611	207
00051801	208
00051802	209
00051811	210
00052201	211
00052202	212
00052211	213
00052401	214
00052402	215
00052411	216
00052601	217
00052602	218
00052611	219
00053201	220
00053202	221
00053211	222

00053701	223
00053711	224
00053901	225
00053902	226
00053911	227
00054401	228
00054402	229
00054411	230
00054601	231
00054602	232
00054611	233
00054801	234
00054802	235
00054811	236
00055301	237
00055302	238
00055311	239
00055501	240
00055502	241
00055511	242
00055701	243
00055702	244
00055711	245
00055901	246
00055902	247
00055911	248
00056401	249
00056402	250
00056411	251
00056601	252
00056602	253
00056611	254
00058601	255
00058602	256
00058611	257
00059801	258
00059802	259
00059811	260
00060001	261
00060002	262

00060011	263
00060201	264
00060202	265
00060211	266
00061201	267
00061202	268
00061211	269
00061401	270
00061402	271
00061411	272
00061801	273
00061802	274
00061811	275
00062001	276
00062002	277
00062011	278
00062201	279
00062202	280
00062211	281
00062401	282
00062402	283
00062411	284
00063401	285
00063402	286
00063411	287
00064401	288
00064402	289
00064411	290
00065002	291
00065501	292
00065502	293
00065511	294
00068001	295
00068002	296
00068011	297
00068301	298
00068302	299
00068311	300
00068401	301
00068402	302

00068411	303
00068701	304
00068711	305
00068801	306
00068802	307
00068811	308
00090001	309
00090002	310
00090011	311
00090101	312
00090102	313
00090111	314
00091101	315
00091102	316
00091111	317
00093001	318
00093002	319
00093011	320
00093501	321
00093502	322
00093511	323
10000009	324
10000010	325
10000011	326
10000012	327
10000013	328
10000014	329
10000015	330
10000016	331
10000017	333
10000018	335
10000019	336
10000020	337
10000021	338
10000022	339
10000023	341
10000027	344
10000028	345
11001008	346
11002003	347

11002004	349
11003601	350
11004002	351
11004601	353
11004602	354
11004603	355
11004605	357
11004606	358
11004608	359
11005901	361
11006004	365
11006005	367
11006006	369
11006701	371
19999496	372
19999497	374
19999498	375
Attack	376
Attack log fields	380
SSL/TLS error messages	383
Traffic	386

Introduction

This document is a detailed reference of all of your FortiWeb appliance's possible log messages. It is organized primarily by the log type:

- [Event](#)
- [Attack](#)
- [Traffic](#)

To look up the meaning of a specific log message, go to the section that matches its *Type* (`type`) field, then look for the table that matches its *ID* (`log_id`).

This document also explains the general structure of FortiWeb log messages, and the meanings of common fields (see [“How to interpret FortiWeb logs” on page 15](#)).

Scope

This document provides administrators information about log messages that can be recorded by a FortiWeb appliance.

This document does **not** cover how to configure logging. It assumes you have already configured it, and need to know how to interpret the log messages. For instructions on how to configure logging, see the [FortiWeb Administration Guide](#) or [FortiWeb CLI Reference](#).

What's new

The list below contains features new or changed since FortiWeb 5.2.

FortiWeb 5.3

- **Messages related to server policy architecture** — To support the new server policy configuration, some event log messages have been removed or replaced. For example, because you now define physical and domain servers within a server pool configuration only, FortiWeb no longer generates log messages for physical or domain server configuration tasks.

For complete information about the architecture changes, see the [FortiWeb Administration Guide](#).

- **Messages for new configuration items** — FortiWeb generates event log messages for configuration tasks related to new features, including:
 - Server pool session persistence
 - SNI (Server Name Indicator)
 - IP reputation exceptions by geolocation
 - Anti-defacement file filter

See [“Event” on page 26](#).

- **Content routing and server pool information in attack and traffic log messages** — Traffic and attack log messages now identify both any HTTP content routing policy FortiWeb applied to the traffic and the server pool FortiWeb routed the traffic to. See [“Header & body fields” on page 15](#).
- **Shorter msg field when disk log is full** — The `msg` log field now has the lowest priority in the disk log. When the total size of all the log fields exceeds the disk log size limit, FortiWeb truncates the msg field, which helps preserve other log information.
- **Time offset calculation** — To improve the accuracy of log search results, FortiWeb now uses the time zone attribute to determine an absolute time offset when it is indexing messages.
- **Attack logs**
 - **HTTP protocol constraint attack log message** — The attack log message that FortiWeb generates when traffic violates a HTTP protocol constraint now provides more information about the violation, including the name of the protection profile that applied the constraint, the specific constraint, and details such as the allowed and detected values.
 - **Cookie poisoning attack log message** — The attack log message that FortiWeb generates when it detects cookie poisoning now shows the expected cookie value and actual value. In addition, it provides the cookie path and domain information.

See [“Attack” on page 376](#).

FortiWeb 5.2

- **Source Country field** — Attack and traffic logs now contain a field (`srccountry`) that identifies the country that is the source of the traffic. See [“Header & body fields” on page 15](#).
- **Signature ID and Signature Subclass Type fields** — Attack logs now contain fields that provide the unique identifier (`signature_id`) and subclass type (`signature_subclass`) of the signature associated with the attack event. See [“Header & body fields” on page 15](#).
- **Custom policy and rule** — Event log messages for access control configuration now refer to `custom-rule` instead of `custom-access-rule` and `custom-policy` instead of `custom-access-policy`. For example, see the message for log [00068001](#).
- **HTTP/HTTPS protocol constraints attack log aggregation** — FortiWeb now records violations of HTTP/HTTPS protocol constraints rules periodically instead of generating a log message for each violation. See [“Attack” on page 376](#).

How to interpret FortiWeb logs

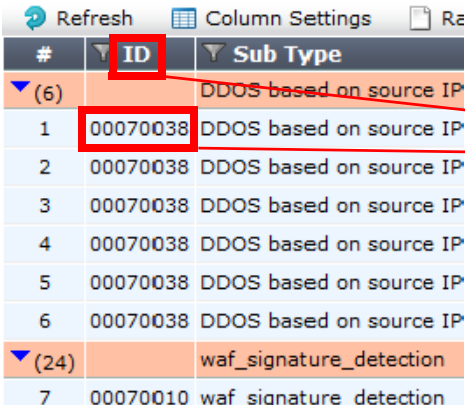
This section explains the composition of FortiWeb log messages.

In some cases, to avoid flooding attack logs with entries, FortiWeb collects multiple attack log messages into a single message. See [“Attack” on page 376](#).

Header & body fields

Each log message is comprised of several field-value pairs. (The names may vary slightly between *Raw* versus *Formatted* views in the web UI.)

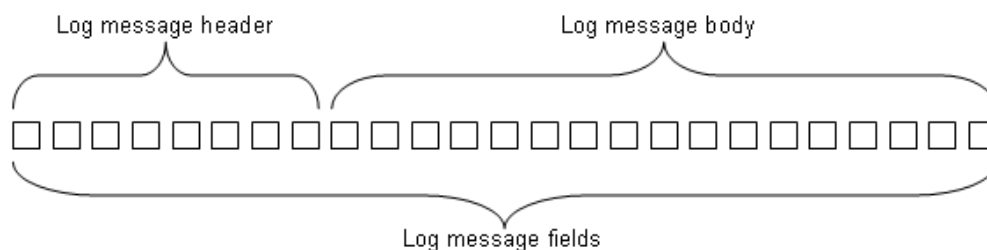
Figure 1: ID (log_id) header field and its value

Formatted view		Raw format	
		log_id=	0104012345
Field name			
Field value			

All log messages' fields belong to one of two parts:

- **Header** — Contains the time and date the log originated, a log identifier, a message identifier, the administrative domain (ADOM), the type of log, the severity level (priority) and where the log message originated. ***These fields exist in all logs.***
- **Body** — Describes the reason why the log was created, plus any actions that the FortiWeb appliance took to respond to it. ***These fields vary by log type.***

Figure 2: Log message header and body



For example, this is a raw-format event log message. Body fields are in ***bold-italic***.

```
date=2013-10-07 time=11:30:53 log_id=10000017 msg_id=000000001117
device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00) Eastern
Time(US & Canada)" type=event subtype="system" pri=information
trigger_policy="" user=admin ui=GUI action=login status=success
msg="User admin login successfully from GUI(172.20.120.47)"
```

This attack log message contains the same header fields, but its body fields are different.

```
date=2014-06-22 time=23:52:38 log_id=20000010 msg_id=000000102972
device_id=FV-1KD3A14800059 vd="root" timezone="(GMT-8:00) Pacific
Time(US&Canada)" type=attack subtype="waf_signature_detection"
pri=alert trigger_policy="" severity_level=Low proto=tcp
service=http action=Alert policy="Auto-policy" src=10.0.8.103
src_port=1114 dst=10.20.8.22 dst_port=80 http_method=get
http_url="/" http_host="10.0.8.22" http_agent="Mozilla/4.0
(compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET4.0C;
.NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; "
http_session_id=none msg="[Signatures name: FWB_server_protection]
[main class name: Information Disclosure] [sub class name: HTTP
Header Leakage]: 080200004" signature_subclass="HTTP Header Leakage"
signature_id="080200004" srccountry="Reserved"
content_switch_name="none" server_pool_name="Auto-ServerFarm"
```

Similarly, traffic log body fields are different.

```
date=2014-06-26 time=00:43:37 log_id=300000000 msg_id=000001351251
device_id=FV-1KD3A14800059 vd="root" timezone="(GMT-8:00) Pacific
Time(US&Canada)" type=traffic subtype="http" pri=notice proto=tcp
service=http status=success reason=none policy=Auto-policy
src=10.0.8.103 src_port=8142 dst=10.20.8.22 dst_port=80
http_request_time=0 http_response_time=0 http_request_bytes=444
http_response_bytes=401 http_method=get http_url="/"
http_host="10.0.8.22" http_agent="Mozilla/4.0 (compatible; MSIE 8.0;
Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727;
.NET CLR 3.0.4506.2152; " http_retcode=200 msg="HTTP GET request from
10.0.8.103:8142 to 10.20.8.22:80" srccountry="Reserved"
content_switch_name="testa" server_pool_name="Auto-ServerFarm"
```

The following table describes each possible header or body field, according to its name as it appears in the *Formatted* or *Raw* view.

Table 1: Log message fields

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Event	Attack	Traffic	
Header					
Date (date)	The year, month, and day when the log message was recorded.	+	+	+	date=2013-10-08
Time (time)	The hour (according to a 24-hour clock, where 15:00 is 3:00 PM), minute, and second that the log message was recorded.	+	+	+	time=15:38:01
ID (log_id)	See “Log ID numbers” on page 23.	+	+	+	log_id=00041101
MSG ID (msg_id)	See “Message IDs” on page 25.	+	+	+	msg_id=0000000000153
Device ID (device_id)	The identifier, typically the serial number, of the appliance which originally recorded the log.	+	+	+	device_id=FV-1KD2B34567890
ADOM (vd)	The administrative domain (ADOM) in which the log message was recorded	+	+	+	vd="root"
Time Zone (timezone)	The name, geographical region, and Greenwich Mean Time (GMT) adjustment of the time zone in which the appliance is located.	+	+	+	timezone=" (GMT-5:00) Eastern Time (US & Canada) "
Type (type)	See “Types” on page 23.	+	+	+	type=event
Sub Type (subtype)	See “Subtypes” on page 24.	+	+	+	subtype=admin
Level (pri)	See “Priority level” on page 24.	+	+	+	pri=alert
Body					
Protocol (proto)	tcp The protocol used by web traffic. By definition, for FortiWeb, this is always TCP.	-	+	+	proto=tcp

Table 1: Log message fields

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Event	Attack	Traffic	
<i>Service</i> (service)	http or https The name of the application-layer protocol used by the traffic. By definition, for FortiWeb, this is always HTTP or HTTPS.	-	+	+	service=http
<i>Source</i> (src)	The IP address of the traffic's origin. The source varies by the direction: <ul style="list-style-type: none"> In HTTP requests, this is the web browser or other client. In HTTP responses, this is the physical server. 	-	+	+	scr=10.0.0.0
<i>Source Port</i> (src_port)	The port number of the traffic's origin.	-	+	+	src_port=3471
<i>Destination</i> (dst)	The IP address of the traffic's destination. The source varies by the direction: <ul style="list-style-type: none"> In HTTP requests, this is the physical server. In HTTP responses, this is the web browser or other client. 	-	+	+	dst=10.0.0.1
<i>Destination Port</i> (dst_port)	The port number of the traffic's destination.	-	+	+	dst_port=8080
<i>Policy</i> (policy)	The name of the server policy governing the traffic which caused the log message.	-	+	+	policy="policy1"
<i>User</i> (user)	The daemon or name of the administrator account that performed the action that caused the log message.	+	-	-	user=admin

Table 1: Log message fields

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Event	Attack	Traffic	
<i>User Interface</i> (ui)	<p>The type of management interface used by the administrative session which caused the log message. Either:</p> <ul style="list-style-type: none"> GUI sshd telnet console none <p>Unless the user is a daemon (which don't have a user interface), logins from <code>none</code> indicate that an administrator used the JavaScript <i>CLI Console</i> widget on <i>System > Status > Status</i> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.</p> <p>Logins from <code>console</code> indicate use of CLI via the local serial console port.</p>	+	-	-	ui=GUI
<i>Action</i> (action)	<p>The action associated with the log message or policy violation, such as:</p> <p>login</p> <p>or</p> <p>Alert</p>	+	+	-	action=Alert
<i>Status</i> (status)	The result of the action.	+	-	+	status=failure
<i>Reason</i> (reason)	The reason for the status, if any.	+	-	+	reason=name_invalid
<i>Return Code</i> (http_retcode)	The HTTP return code. If FortiWeb is configured to redirect, this is the rewritten code, not the original one from the server.	-	-	+	http_retcode=200
<i>Request Time</i> (http_request_time)	The amount of time it took FortiWeb to process the client request, in milliseconds (ms).	-	-	+	http_request_time=10

Table 1: Log message fields

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Event	Attack	Traffic	
<i>Response Time</i> (http_response_time)	The amount of processing time for the response in milliseconds (ms). This can be a useful measure of performance issues, especially if processing involves regular expressing matching.	-	-	+	http_response_time=10
<i>Request Bytes</i> (http_request_bytes)	The size of the request in bytes.	-	-	+	http_request_bytes=2
<i>Response Bytes</i> (http_response_bytes)	The size of the individual response in bytes (B). For chunked responses, this is for each reply; it does not aggregate all related chunks.	-	-	+	http_response_bytes=136
<i>Method</i> (http_method)	The method, such as GET or POST, used by the HTTP request.	-	+	+	http_method=get
<i>URL</i> (http_url)	The URL in the HTTP header of the original HTTP request, such as: <code>/images/buttons/hintOver.png</code> This does not include the service (http://) nor host name (example.nl). If FortiWeb is configured to rewrite the URL, this is the original URL from the client, not the rewritten one.	-	+	+	http_url="/image/up.png"

Table 1: Log message fields

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Event	Attack	Traffic	
<i>Host</i> (http_host)	<p>The <code>Host :</code> field in the HTTP header of the HTTP request, such as:</p> <p><code>www.example.com</code></p> <p>or</p> <p><code>10.0.0.1:8080</code></p> <p>This is typically a fully qualified domain name (FQDN) or IP address and port number that resolves or routes to the virtual server on the FortiWeb appliance.</p> <p>This may be different from your internal DNS name (if any) for the web server, or, if you are using HTTP <code>Host :</code> rewrites, different from the virtual host on the web server. For example, this might be <code>www.example.co.jp</code> instead of <code>www1.local</code> or the virtual host that serves responses for all DNS names, <code>www.example.com</code>.</p>	-	+	+	<code>http_host="example.com"</code>
<i>User Agent</i> (http_agent)	The name and version of the HTTP client, usually a web browser. This is reported by the client itself in the <code>User-Agent :</code> HTTP header. In attacks, it is often fake.	-	+	+	<code>http_agent="Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.110 Safari/537.36"</code>
<i>FortiWeb Session ID</i> (http_session_id)	<p>The session identifier for a client's related HTTP requests (if any).</p> <p>The ID may be unknown if the <i>Session Management</i> option is not enabled in the applied protection profile, and therefore FortiWeb has not injected a session cookie nor inferred a session ID from the protected web application.</p>	-	+	-	<code>http_session_id=K8BXT3TNYUM710UEGWC8IQBTPX9PRWHB</code>
<i>Severity Level</i> (severity_level)	The severity that the administrator configured in the rule or policy governing the traffic which caused the log message.	-	+	-	<code>severity_level=High</code>

Table 1: Log message fields

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Event	Attack	Traffic	
<i>Trigger Policy</i> (trigger_policy)	The name of the notification servers used to record and/or deliver this log message (if any). The trigger policy value may be an empty string if no trigger policy was selected.	-	+	-	trigger_policy=notification-server-group1
<i>Signature Subclass</i> (signature_subclass)	The name of the signature subclass. If the current signature has no subclass, the main class is displayed.	-	+	-	"Cross Site Scripting"
<i>Signature ID</i> (signature_id)	The ID of the specific signature within the subclass that triggered the log message.	-	+	-	"010000001"
<i>Source Country</i> (srccountry)	The country that is the source of the traffic.	-	+	+	"United States"
<i>Message</i> (msg)	Details describing the reason why the log message was created. The message varies by the nature of the cause. The msg log field has the lowest priority in the disk log. When the total size of all the log fields exceeds the disk log size limit, FortiWeb truncates the msg field, which helps preserve other log information.	+	+	+	msg="User admin changed dns from GUI (172.20.120.47) "
<i>HTTP Content Routing</i> (content_switch_name)	The name of the associated HTTP content routing policy.	-	+	+	content_switch_name="httproutes1"

Table 1: Log message fields

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Event	Attack	Traffic	
<i>Server Pool</i> (server_pool_name)	The name of the server pool in the associated server policy.	-	+	+	server_pool_name="Auto-ServerFarm"
<i>Detailed Information</i> (N/A)	<p>This column contains the entire log message in raw format.</p> <p>If your <i>Column Settings</i> show this column, the entire raw log message will be included in the row under this column, next to the formatted column view of the same log message. This way, if you want to view the entire raw log message, you can simply scroll the page, instead of switching the entire page back and forth from <i>Raw</i> to <i>Formatted</i> log views.</p> <p>This column appears only when using the <i>Formatted</i> log view. It does not actually exist as a field in the raw logs.</p>	+	+	+	date=2013-10-10 time=00:38:58 log_id=20000051 msg_id=0000000000008...

Log ID numbers

The *ID* (log_id) is an 8-digit field located in the header, immediately following the time and date fields.

The log_id field is a number assigned to all permutations of the same message. It classifies a log message by the nature of the cause of the log message, such as administrator authentication failures or traffic. Other log messages that share the same cause will share the same log_id.

For example, creating an administrator account always has the log ID [00003401](#).

Types

Each log message contains a *Type* (type) field that indicates its category, and in which log file it is stored.

FortiWeb appliances can record the following categories of log messages:

Table 2: Log types

Log type	Description
----------	-------------

Table 2: Log types

Event	Records system and administrative events, such as downloading a backup copy of the configuration, or daemon activities.
Traffic	Records traffic flow information, such as an HTTP/HTTPS request and its response, if any.
Attack	Records attack and intrusion attempts.



Avoid recording highly frequent log types such as traffic logs to the local hard disk for an extended period of time. **Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.**

Subtypes

Each log message contains a *Sub Type* (subtype) field that further subdivides its category according to the feature involved with the cause of the log message.

For example:

- In event logs, some may have a subtype of [admin](#), [system](#), or other subtypes.
- In attack logs, some may have a subtype of [waf_padding_oracle](#) or other subtypes.
- In traffic logs, the subtype is always [http](#) **even if the service is HTTPS**.

Priority level

Each log message contains a *Level* (pri) field that indicates the estimated severity of the event that caused the log message, such as pri=warning, and therefore how high a priority it is likely to be.



Level (pri) associations with the descriptions below are not always uniform. They also may not correspond with **your own** definitions of how severe each event is. If you require notification when a specific event occurs, either configure SNMP traps or alert email by administrator-defined *Severity Level* (severity_level) or *ID* (log_id), **not** by *Level* (pri).

Table 3: Approximate log priority levels

Level (0 is highest)	Name	Description
0	Emergency	The system has become unusable.
1	Alert	Immediate action is required. Used in attack logs.
2	Critical	Functionality is affected.
3	Error	An error condition exists and functionality could be affected.
4	Warning	Functionality could be affected.

Table 3: Approximate log priority levels

Level (0 is highest)	Name	Description
5	Notification	Information about normal events. <i>Used in traffic logs, and in event logs for administrator logins, time changes, and normal daemon actions.</i>
6	Information	General information about system operations. <i>Used in event logs for configuration changes.</i>

For each location where the FortiWeb appliance can store log files (disk, memory, Syslog or FortiAnalyzer), you can define a severity threshold. The FortiWeb appliance will store all log messages equal to or exceeding the log severity level you select.

For example, if you select *Error*, the FortiWeb appliance will store log messages whose log severity level is *Error*, *Critical*, *Alert*, and *Emergency*.



Avoid recording log messages using low log severity thresholds such as information or notification to the local hard disk for an extended period of time. A low log severity threshold is one possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

Message IDs

The *MSG ID* (`msg_id`) field is an 12-digit number located in the header, incremented with each individual log message generated by the FortiWeb appliance. It is used only for numbering each entry in the database, and does not necessarily reflect its cause.

Each `msg_id` number is a unique identifier for that specific log entry. No other log messages, regardless of cause, share the same `msg_id`.

Event

Event log messages record subsystem events such as NTP-based time changes, reboots and RAID level changes. They also record configuration changes.

Unless noted as otherwise in each event log's description:

- *Level* (*pri*) field is *information*
- *User* (*user*) field is the name of the administrator account that caused the event
- *User Interface* (*ui*) field is according to [“User Interface” on page 19](#)

To go to a sample, additional information, and solution (if applicable) for an event log message, click the *ID* (*log_id*) field in [Table 4](#).

Table 4: Event logs by subtype & ID

ID (log_id)	Sub Type (subtype)
00001002	admin
00001012	admin
00001052	admin
00001062	admin
00002202	admin
00002801	admin
00002802	admin
00002811	admin
00003401	admin
00003402	admin
00003411	admin
00004401	admin
00004402	admin
00004411	admin
00004902	admin
00006001	admin
00006002	admin
00006011	admin
00006102	admin

Table 4: Event logs by subtype & ID

ID (log_id)	Sub Type (subtype)
00006202	admin
00006302	admin
00006501	admin
00006502	admin
00006511	admin
00007302	admin
00007402	admin
00008101	admin
00008102	admin
00008111	admin
00008602	admin
00008701	admin
00008702	admin
00008711	admin
00008801	admin
00008811	admin
00008901	admin
00008911	admin
00009001	admin
00009011	admin
00009101	admin
00009111	admin
00009201	admin
00009211	admin
00009301	admin
00009311	admin
00009401	admin
00009402	admin

Table 4: Event logs by subtype & ID

ID (log_id)	Sub Type (subtype)
00009411	admin
00009501	admin
00009502	admin
00009511	admin
00009702	admin
00010001	admin
00010002	admin
00010011	admin
00010201	admin
00010202	admin
00010211	admin
00010401	admin
00010402	admin
00010411	admin
00010501	admin
00010502	admin
00010511	admin
00010601	admin
00010602	admin
00010611	admin
00010701	admin
00010711	admin
00020088	admin
00020201	admin
00020202	admin
00020211	admin
00020301	admin
00020302	admin

Table 4: Event logs by subtype & ID

ID (log_id)	Sub Type (subtype)
00020311	admin
00020801	admin
00020802	admin
00020811	admin
00020901	admin
00020902	admin
00020911	admin
00021002	admin
00021102	admin
00021140	admin
00021202	admin
00021302	admin
00021402	admin
00022997	admin
00030001	admin
00030002	admin
00030011	admin
00032006	admin
00040001	admin
00040002	admin
00040011	admin
00040301	admin
00040302	admin
00040311	admin
00040501	admin
00040502	admin
00040511	admin
00040601	admin

Table 4: Event logs by subtype & ID

ID (log_id)	Sub Type (subtype)
00040611	admin
00040623	admin
00040751	admin
00040752	admin
00040761	admin
00040801	admin
00040802	admin
00040811	admin
00040901	admin
00040902	admin
00040911	admin
00041001	admin
00041002	admin
00041011	admin
00041101	admin
00041102	admin
00041111	admin
00041201	admin
00041202	admin
00041211	admin
00041302	admin
00041401	admin
00041402	admin
00041411	admin
00041601	admin
00041602	admin
00041611	admin
00041801	admin

Table 4: Event logs by subtype & ID

ID (log_id)	Sub Type (subtype)
00041802	admin
00041811	admin
00043001	admin
00043002	admin
00043011	admin
00044001	admin
00044002	admin
00044011	admin
00044401	admin
00044411	admin
00044501	admin
00044502	admin
00044511	admin
00046001	admin
00046002	admin
00046011	admin
00050001	admin
00050002	admin
00050011	admin
00050201	admin
00050202	admin
00050211	admin
00050401	admin
00050402	admin
00050411	admin
00051001	admin
00051002	admin
00051011	admin

Table 4: Event logs by subtype & ID

ID (log_id)	Sub Type (subtype)
00051201	admin
00051202	admin
00051211	admin
00051401	admin
00051402	admin
00051411	admin
00051601	admin
00051602	admin
00051611	admin
00051801	admin
00051802	admin
00051811	admin
00052201	admin
00052202	admin
00052211	admin
00052401	admin
00052402	admin
00052411	admin
00052601	admin
00052602	admin
00052611	admin
00053201	admin
00053202	admin
00053211	admin
00053701	admin
00053711	admin
00053901	admin
00053902	admin

Table 4: Event logs by subtype & ID

ID (log_id)	Sub Type (subtype)
00053911	admin
00054401	admin
00054402	admin
00054411	admin
00054601	admin
00054602	admin
00054611	admin
00054801	admin
00054802	admin
00054811	admin
00055301	admin
00055302	admin
00055311	admin
00055501	admin
00055502	admin
00055511	admin
00055701	admin
00055702	admin
00055711	admin
00055901	admin
00055902	admin
00055911	admin
00056401	admin
00056402	admin
00056411	admin
00056601	admin
00056602	admin
00056611	admin

Table 4: Event logs by subtype & ID

ID (log_id)	Sub Type (subtype)
00058601	admin
00058602	admin
00058611	admin
00059801	admin
00059802	admin
00059811	admin
00060001	admin
00060002	admin
00060011	admin
00060201	admin
00060202	admin
00060211	admin
00061201	admin
00061202	admin
00061211	admin
00061401	admin
00061402	admin
00061411	admin
00061801	admin
00061802	admin
00061811	admin
00062001	admin
00062002	admin
00062011	admin
00062201	admin
00062202	admin
00062211	admin
00062401	admin

Table 4: Event logs by subtype & ID

ID (log_id)	Sub Type (subtype)
00062402	admin
00062411	admin
00063401	admin
00063402	admin
00063411	admin
00064401	admin
00064402	admin
00064411	admin
00065002	admin
00065501	admin
00065502	admin
00065511	admin
00068001	admin
00068002	admin
00068011	admin
00068301	admin
00068302	admin
00068311	admin
00068401	admin
00068402	admin
00068411	admin
00068701	admin
00068711	admin
00068801	admin
00068802	admin
00068811	admin
00090001	admin
00090002	admin

Table 4: Event logs by subtype & ID

ID (log_id)	Sub Type (subtype)
00090011	admin
00090101	admin
00090102	admin
00090111	admin
00091101	admin
00091102	admin
00091111	admin
00093001	admin
00093002	admin
00093011	admin
00093501	admin
00093502	admin
00093511	admin
10000009	system
10000010	system
10000011	system
10000012	system
10000013	system
10000014	system
10000015	system
10000016	system
10000017	system
10000018	system
10000019	system
10000020	system
10000021	system
10000022	system
10000023	system

Table 4: Event logs by subtype & ID

ID (log_id)	Sub Type (subtype)
10000027	system
10000028	system
11001008	system
11002003	system
11002004	system
11003601	system
11004002	system
11004601	system
11004602	system
11004603	system
11004605	system
11004606	system
11004608	system
11005901	system
11006004	system
11006005	system
11006006	system
11006701	system
19999496	system
19999497	system
19999498	system

Reboot, shut down, & boot up messages

When FortiWeb is shutting down, if you are attached to the local console, the appliance outputs messages output to the CLI notifying you that the operating system is halting, such as:

```
The system is going down NOW !!
```

or:

```
System is rebooting...
```

As one of its final actions, if logging is enabled, FortiWeb records the shutdown ([10000011](#)) or reboot ([10000010](#)) in the event log. When FortiWeb starts up again, the local console displays:

```
System is started.
```

and it records the startup ([10000009](#)). Its subsystems are loaded and readied to do their work. At this time FortiWeb records daemon startups in the event log, such as [10000023](#) and [11001008](#).

Related

- [10000009](#)
- [10000010](#)
- [10000011](#)
- [10000023](#)
- [11001008](#)

Table 5:

Meaning
<p>Either:</p> <ul style="list-style-type: none"> • An administrator changed the NTP synchronization interval. • An administrator changed the time zone setting.

Table 6:

Field name	Description
ID (log_id)	00001002 See “Log ID numbers” on page 23.
Level (pri)	notification or information See “Priority level” on page 24.

Table 7:

Examples
<pre>date=2014-04-09 time=22:11:33 log_id=00001002 msg_id=000000192626 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=notice trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed a time setting from GUI(172.22.6.240)"</pre>

Related

- [00021140](#)
- [00006102](#)

00001012

Table 8:

Meaning
<ul style="list-style-type: none">A FortiWeb administrator changed the host name of the appliance.

Table 9:

Field name	Description
ID (log_id)	00001012 See “Log ID numbers” on page 23.
Level (pri)	notification or information (changing the idle GUI session timeout) See “Priority level” on page 24.

Table 10:

Examples
<pre>date=2014-04-10 time=12:11:17 log_id=00001012 msg_id=000000192621 device_id=FV-1KD3A13800012 vd="root" timezone=" (GMT+8:00) Beijing, ChongQing, HongKong, Urumgi" type=event subtype="admin" pri=notice trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed hostname global setting FortiWeb to 1KD_1 from GUI(172.22.6.240) "</pre>

Related

- [00001002](#)

00001052

Table 11:

Meaning
<ul style="list-style-type: none">An administrator changed the idle GUI session timeout.

Table 12:

Field name	Description
ID (log_id)	00001052 See “Log ID numbers” on page 23.
Level (pri)	notification or information (changing the idle GUI session timeout) See “Priority level” on page 24.

Table 13:

Examples
<pre>date=2014-04-10 time=12:10:51 log_id=00001052 msg_id=000000192620 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=notice trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed idle GUI session timeout from GUI(172.22.6.240)"</pre>

Related

- [00001002](#)

Table 14:

Meaning
<ul style="list-style-type: none"> An administrator changed the listening/source port for configuration synchronization with another FortiWeb.

Table 15:

Field name	Description
ID (log_id)	00001062 See “Log ID numbers” on page 23.
Level (pri)	notice See “Priority level” on page 24.

Table 16:

Examples
<pre>date=2014-09-10 time=22:16:40 log_id=00001062 msg_id=000003041952 device_id=FV400C3M14000006 vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=notice trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed sync-port global setting 8333 to 1111 from GUI(172.22.14.6) "</pre>

Related

- [00001002](#)

00002202

Table 17:

Meaning
A FortiWeb administrator changed a setting in <i>System > Config > Advanced</i> on the appliance.

Table 18:

Field name	Description
ID (log_id)	00002202 See “Log ID numbers” on page 23.

Table 19:

Example
<pre>date=2013-10-08 time=09:43:22 log_id=00002202 msg_id=0000000000042 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed advanced from GUI(172.20.120.47) "</pre>

00002801

Table 20:

Meaning
A FortiWeb administrator created an administrator access profile.

Table 21:

Field name	Description
ID (log_id)	00002801 See “Log ID numbers” on page 23.

Table 22:

Example
<pre>date=2013-10-08 time=09:43:04 log_id=00002801 msg_id=00000000000041 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added accprofile read-only from GUI(172.20.120.47) "</pre>

Related

- [00002802](#)
- [00002811](#)
- [00003401](#)

Table 23:

Meaning
A FortiWeb administrator changed an administrator access profile.

Table 24:

Field name	Description
ID (log_id)	00002802 See “Log ID numbers” on page 23.

Table 25:

Example
<pre>date=2013-10-08 time=09:43:14 log_id=00002802 msg_id=0000000000042 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed accprofile read-only from GUI(172.20.120.47) "</pre>

Related

- [00002801](#)
- [00002811](#)
- [00003401](#)

00002811

Table 26:

Meaning
A FortiWeb administrator deleted an administrator access profile.

Table 27:

Field name	Description
ID (log_id)	00002811 See “Log ID numbers” on page 23.

Table 28:

Example
<pre>date=2013-10-08 time=09:43:34 log_id=00002811 msg_id=0000000000045 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted accprofile read-only from GUI(172.20.120.47) "</pre>

Related

- [00002801](#)
- [00002802](#)
- [00003401](#)

00003401

Table 29:

Meaning
A FortiWeb administrator created an administrator account.

Table 30:

Field name	Description
ID (log_id)	00003401 See “Log ID numbers” on page 23.

Table 31:

Example
<pre>date=2013-10-08 time=09:45:44 log_id=00003401 msg_id=0000000000048 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added admin admin1 from GUI(172.20.120.47) "</pre>

Related

- [00003402](#)
- [00003411](#)
- [00002801](#)
- [00004402](#)
- [00010201](#)
- [00010401](#)
- [00010701](#)

Table 32:

Meaning
A FortiWeb administrator changed an administrator account. This can include resetting the account's password.

Table 33:

Field name	Description
ID (log_id)	00003402 See “Log ID numbers” on page 23 .

Table 34:

Example
<code>date=2013-10-08 time=09:45:44 log_id=00003402 msg_id=0000000000049 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed admin admin1 from GUI(172.20.120.47) "</code>

Related

- [00003401](#)
- [00003411](#)
- [00002801](#)
- [00010201](#)
- [00010401](#)
- [00010701](#)

00003411

Table 35:

Meaning
A FortiWeb administrator deleted an administrator account.

Table 36:

Field name	Description
ID (log_id)	00003411 See “Log ID numbers” on page 23.

Table 37:

Example
<pre>date=2013-10-08 time=09:46:44 log_id=00003411 msg_id=00000000000052 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted admin admin1 from GUI(172.20.120.47) "</pre>

Related

- [00003401](#)
- [00003402](#)
- [00002801](#)

00004401

Table 38:

Meaning
A FortiWeb administrator created a VLAN subinterface or link aggregate.

Table 39:

Field name	Description
ID (log_id)	00004401 See “Log ID numbers” on page 23 .

Table 40:

Examples
<pre>date=2013-10-06 time=11:00:13 log_id=00004401 msg_id=0000000001083 device_id=FVVM0400000010871 vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=add status=success msg="User admin added interface vlan3 from console"</pre>

Related

- [00004402](#)
- [00030001](#)
- [00030011](#)
- [11006004](#)

Table 41:

Meaning
A FortiWeb administrator changed the IP address or allowed administrative access protocols of a network interface. This does not include bringing up or bringing down the interface (see 11006004).

Table 42:

Field name	Description
ID (log_id)	00004402 See “Log ID numbers” on page 23.
Sub Type (subtype)	admin See “Subtypes” on page 24.
Level (pri)	information See “Priority level” on page 24.
User (user)	<administrator_name>
User Interface (ui)	{GUI none telnet ssh console} Logins from jsconsole indicate use of the <i>CLI Console</i> widget on <i>System > Status > Status</i> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Message (msg)	User <administrator_name> changed interface <interface_name> from {GUI(<mgmt_ip>) none telnet(<mgmt_ip>) ssh(<mgmt_ip>) console}

Table 43:

Examples
date=2013-10-06 time=11:00:19 log_id=00004402 msg_id=000000001085 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=edit status=success msg="User admin changed interface port1 from console"

Related

- [00003401](#)
- [00004401](#)
- [00006202](#)
- [00030001](#)
- [00030011](#)
- [11006004](#)

Table 44:

Meaning
A FortiWeb administrator deleted a VLAN subinterface or link aggregate.

Table 45:

Field name	Description
ID (log_id)	00004411 See “Log ID numbers” on page 23.
Sub Type (subtype)	admin See “Subtypes” on page 24.
Level (pri)	information See “Priority level” on page 24.
User (user)	<administrator_name>
User Interface (ui)	{GUI none telnet ssh console} Logins from jsconsole indicate use of the <i>CLI Console</i> widget on <i>System > Status > Status</i> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Message (msg)	User <administrator_name> changed interface <interface_name> from {GUI(<mgmt_ip>) none telnet(<mgmt_ip>) ssh(<mgmt_ip>) console}

Table 46:

Examples
date=2013-10-06 time=11:00:19 log_id=00004411 msg_id=000000001089 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=delete status=success msg="User admin deleted interface agg1 from console"

Related

- [00004401](#)
- [00004402](#)
- [00030001](#)
- [00030011](#)
- [11006004](#)

Table 47:

Meaning
A FortiWeb administrator changed the operation mode.

Table 48:

Field name	Description
ID (log_id)	00004902 See “Log ID numbers” on page 23.
Sub Type (subtype)	admin See “Subtypes” on page 24.
Level (pri)	information See “Priority level” on page 24.
User (user)	<administrator_name>
User Interface (ui)	{GUI(<mgmt_ip>) none telnet(<mgmt_ip>) ssh(<mgmt_ip>) console} Logins from jsconsole indicate use of the <i>CLI Console</i> widget on <i>System > Status > Status</i> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Message (msg)	User <administrator_name> changed settings from {GUI(<mgmt_ip>) none telnet(<mgmt_ip>) ssh(<mgmt_ip>) console}

Table 49:

Example
date=2014-05-14 time=18:05:27 log_id=00004902 msg_id=000000021625 device_id=FV-3KC3R10700108 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed settings from GUI(172.22.6.241) "

Related

- [00006001](#)

00006001

Table 50:

Meaning
A FortiWeb administrator created a bridge ("V-Zone").

Table 51:

Field name	Description
ID (log_id)	00006001 See "Log ID numbers" on page 23.
Sub Type (subtype)	system See "Subtypes" on page 24.
Level (pri)	information See "Priority level" on page 24.
User (user)	<administrator_name>
User Interface (ui)	{GUI(<mgmt_ip>) none telnet(<mgmt_ip>) ssh(<mgmt_ip>) console}
Message (msg)	User <administrator_name> added V-Zone <bridge_name> from {GUI(<mgmt_ip>) jsconsole telnet(<mgmt_ip>) ssh(<mgmt_ip>) console}.

Table 52:

Example
<pre>date=2014-04-20 time=14:59:56 log_id=00090002 msg_id=000000176080 type=event subtype="system" pri=information device_id=FVVM020000003619 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" user=admin ui=GUI(172.20.120.229) msg="User admin added V-Zone bridge1 from GUI(172.20.120.229) ."</pre>

Related

- [00006002](#)
- [00006011](#)

Table 53:

Meaning
A FortiWeb administrator changed a bridge ("V-Zone").

Table 54:

Field name	Description
ID (log_id)	00006002 See "Log ID numbers" on page 23.
Sub Type (subtype)	system See "Subtypes" on page 24.
Level (pri)	information See "Priority level" on page 24.
User (user)	<administrator_name>
User Interface (ui)	{GUI(<mgmt_ip>) none telnet(<mgmt_ip>) ssh(<mgmt_ip>) console}
Message (msg)	User <administrator_name> modified V-Zone <bridge_name> from {GUI(<mgmt_ip>) jsconsole telnet(<mgmt_ip>) ssh(<mgmt_ip>) console}.

Table 55:

Example
date=2014-04-20 time=14:59:56 log_id=00090002 msg_id=000000176080 type=event subtype="system" pri=information device_id=FVVM020000003619 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" user=admin ui=GUI(172.20.120.229) msg="User admin modified V-Zone bridge1 from GUI(172.20.120.229) ."

Related

- [00006001](#)
- [00006011](#)

Table 56:

Meaning
A FortiWeb administrator deleted a bridge ("V-Zone").

Table 57:

Field name	Description
ID (log_id)	00006011 See "Log ID numbers" on page 23.
Sub Type (subtype)	system See "Subtypes" on page 24.
Level (pri)	information See "Priority level" on page 24.
User (user)	<administrator_name>
User Interface (ui)	{GUI(<mgmt_ip>) none telnet(<mgmt_ip>) ssh(<mgmt_ip>) console}
Message (msg)	User <administrator_name> deleted V-Zone <bridge_name> from {GUI(<mgmt_ip>) jsconsole telnet(<mgmt_ip>) ssh(<mgmt_ip>) console}.

Table 58:

Example
date=2014-04-20 time=14:59:56 log_id=00090002 msg_id=000000176080 type=event subtype="system" pri=information device_id=FVVM020000003619 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" user=admin ui=GUI(172.20.120.229) msg="User admin deleted V-Zone bridge1 from GUI(172.20.120.229) ."

Related

- [00006001](#)
- [00006002](#)

00006102

Table 59:

Meaning
A FortiWeb administrator changed the IP address of the configuration synchronization peer.

Table 60:

Field name	Description
ID (log_id)	00006102 See “Log ID numbers” on page 23.

Table 61:

Example
<pre>date=2013-10-08 time=09:47:28 log_id=00006102 msg_id=00000000000060 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed conf-sync from GUI(172.20.120.47) "</pre>

Related

- [00001002](#)

Table 62:

Meaning
A FortiWeb administrator changed the DNS settings.

Table 63:

Field name	Description
ID (log_id)	00006202 See “Log ID numbers” on page 23.

Table 64:

Example
<pre>date=2013-10-08 time=09:47:37 log_id=00006202 msg_id=00000000000061 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed dns from GUI(172.20.120.47) "</pre>

Related

- [00004402](#)
- [00030011](#)

Table 65:

Meaning
A FortiWeb administrator changed the system-wide SNMP settings such as the description, location, or contact information.

Table 66:

Field name	Description
ID (log_id)	00006302 See “Log ID numbers” on page 23.

Table 67:

Example
<code>date=2013-10-08 time=09:44:37 log_id=00006302 msg_id=0000000000044 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed snmpsysinfo from GUI(172.20.120.47) "</code>

Related

- [00004402](#)
- [00006501](#)

Table 68:

Meaning
A FortiWeb administrator added an SNMP community.

Table 69:

Field name	Description
ID (log_id)	00006501 See “Log ID numbers” on page 23.

Table 70:

Example
<pre>date=2013-10-08 time=09:45:04 log_id=00006501 msg_id=00000000000045 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added snmp community 1 from GUI(172.20.120.47)"</pre>

Related

- [00004402](#)
- [00006302](#)
- [00006502](#)
- [00006511](#)

Table 71:

Meaning
A FortiWeb administrator changed an SNMP community settings such as the SNMP manager and trap events.

Table 72:

Field name	Description
ID (log_id)	00006502 See “Log ID numbers” on page 23.

Table 73:

Example
<pre>date=2013-10-08 time=09:45:04 log_id=00006502 msg_id=00000000000046 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed snmp community 1 from GUI(172.20.120.47) "</pre>

Related

- [00004402](#)
- [00006302](#)
- [00006501](#)
- [00006511](#)

00006511

Table 74:

Meaning
A FortiWeb administrator deleted an SNMP community.

Table 75:

Field name	Description
ID (log_id)	00006511 See “Log ID numbers” on page 23.

Table 76:

Example
<pre>date=2013-10-08 time=09:47:11 log_id=00006511 msg_id=0000000000059 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted snmp community 2 from GUI(172.20.120.47) "</pre>

Related

- [00004402](#)
- [00006302](#)
- [00006501](#)
- [00006502](#)

00007302

Table 77:

Meaning
A FortiWeb administrator changed the setting that overrides the default Fortiguard Distribution Server (FDS).

Table 78:

Field name	Description
ID (log_id)	00007302 See “Log ID numbers” on page 23.

Table 79:

Example
<pre>date=2014-04-10 time=00:15:13 log_id=00007302 msg_id=0000000070586 device_id=FV-1KC3R10700031 vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed system-autoupdate-override from GUI(172.22.6.237) "</pre>

Related

- [00007402](#)

00007402

Table 80:

Meaning
A FortiWeb administrator changed the configuration that determines how the FortiWeb appliance accesses the Fortinet Distribution Network (FDN) to retrieve updates.

Table 81:

Field name	Description
ID (log_id)	00007402 See “Log ID numbers” on page 23.

Table 82:

Example
<pre>date=2014-04-10 time=16:19:36 log_id=00007402 msg_id=000000734625 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed system-autoupdate-schedule from GUI(172.22.6.237) "</pre>

Related

- [00007302](#)

00008101

Table 83:

Meaning
A FortiWeb administrator created a schedule for a periodic configuration backup to an FTP/SFTP server.

Table 84:

Field name	Description
ID (log_id)	00008101 See “Log ID numbers” on page 23.

Table 85:

Example
<pre>date=2013-10-08 time=09:42:14 log_id=00008101 msg_id=00000000000037 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added backup scheduled_backup from GUI(172.20.120.47) "</pre>

Related

- [00004402](#)
- [00008102](#)
- [00008111](#)

00008102

Table 86:

Meaning
A FortiWeb administrator changed a schedule for a periodic configuration backup to an FTP/SFTP server.

Table 87:

Field name	Description
ID (log_id)	00008102 See “Log ID numbers” on page 23.

Table 88:

Example
<pre>date=2013-10-08 time=09:42:24 log_id=00008102 msg_id=00000000000038 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed backup scheduled_backup from GUI(172.20.120.47) "</pre>

Related

- [00004402](#)
- [00008101](#)
- [00008111](#)

00008111

Table 89:

Meaning
A FortiWeb administrator deleted a schedule for a periodic configuration backup to an FTP/SFTP server.

Table 90:

Field name	Description
ID (log_id)	00008111 See “Log ID numbers” on page 23.

Table 91:

Example
<pre>date=2013-10-08 time=09:42:54 log_id=00008111 msg_id=0000000000040 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted backup scheduled_backup from GUI(172.20.120.47) "</pre>

Related

- [00004402](#)
- [00008101](#)
- [00008102](#)

00008602

Table 92:

Meaning
A FortiWeb administrator changed a TCP SYN flood denial of service (DoS) setting.

Table 93:

Field name	Description
ID (log_id)	00008602 See “Log ID numbers” on page 23.

Table 94:

Example
<pre>date=2013-10-08 time=10:38:51 log_id=00008602 msg_id=0000000000174 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed dos-prevention from GUI(172.20.120.47) "</pre>

00008701

Table 95:

Meaning
A FortiWeb administrator uploaded a locally stored server certificate and (if applicable) private key.

Table 96:

Field name	Description
ID (log_id)	00008701 See “Log ID numbers” on page 23.

Table 97:

Example
<pre>date=2013-10-08 time=09:42:13 log_id=00008701 msg_id=00000000000039 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added local certificate-with-key from GUI(172.20.120.47) "</pre>

Related

- [00008702](#)
- [00008711](#)

00008702

Table 98:

Meaning
A FortiWeb administrator changed the description of a locally stored server certificate and private key.

Table 99:

Field name	Description
ID (log_id)	00008702 See “Log ID numbers” on page 23.

Table 100:

Example
<pre>date=2013-10-08 time=09:42:53 log_id=00008702 msg_id=0000000000040 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed local certificate-with-key from GUI(172.20.120.47) "</pre>

Related

- [00008701](#)
- [00008711](#)

00008711

Table 101:

Meaning
A FortiWeb administrator deleted a locally stored server certificate and (if applicable) private key.

Table 102:

Field name	Description
ID (log_id)	00008711 See “Log ID numbers” on page 23.

Table 103:

Example
<pre>date=2013-10-08 time=09:42:59 log_id=00008711 msg_id=0000000000041 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted local certificate-with-key from GUI(172.20.120.47) "</pre>

Related

- [00008701](#)
- [00008702](#)

Table 104:

Meaning
A FortiWeb administrator added a configuration for a certificate of the HTTP CRL server of your certificate authority (CA).

Table 105:

Field name	Description
ID (log_id)	00008801 See “Log ID numbers” on page 23.

Table 106:

Example
<pre>date=2014-04-10 time=17:01:21 log_id=00008801 msg_id=000000179544 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added remote REMOTE_Cert_2 from GUI(172.22.6.66) "</pre>

Related

- [00008811](#)
- [00009301](#)
- [00009311](#)
- [11006701](#)

00008811

Table 107:

Meaning
A FortiWeb administrator deleted a configuration for a certificate of the HTTP CRL server of your certificate authority (CA).

Table 108:

Field name	Description
ID (log_id)	00008811 See “Log ID numbers” on page 23 .

Table 109:

Example
<pre>date=2014-04-10 time=17:02:34 log_id=00008811 msg_id=000000179545 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted remote REMOTE_Cert_2 from GUI(172.22.6.66) "</pre>

Related

- [00008801](#)
- [00009301](#)
- [00009311](#)
- [11006701](#)

Table 110:

Meaning
A FortiWeb administrator added a certificate.

Table 111:

Field name	Description
ID (log_id)	00008901 See “Log ID numbers” on page 23.

Table 112:

Example
<pre>date=2014-04-10 time=17:03:26 log_id=00008901 msg_id=000000179546 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added certificate ca CA_Cert_4 from GUI(172.22.6.66) "</pre>

Related

- [00008911](#)

Table 113:

Meaning
A FortiWeb administrator deleted a certificate.

Table 114:

Field name	Description
ID (log_id)	00008911 See “Log ID numbers” on page 23.

Table 115:

Example
<pre>date=2014-04-10 time=17:03:31 log_id=00008911 msg_id=000000179547 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted certificate ca CA_Cert_4 from GUI(172.22.6.66) "</pre>

Related

- [00008901](#)

00009001

Table 116:

Meaning
A FortiWeb administrator added a certificate authorities (CA) group.

Table 117:

Field name	Description
ID (log_id)	00009001 See “Log ID numbers” on page 23.

Table 118:

Example
<pre>date=2014-04-10 time=17:06:20 log_id=00009001 msg_id=000000179548 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added certificate ca-group ca_g from GUI(172.22.6.66) "</pre>

Related

- [00009011](#)

00009011

Table 119:

Meaning
A FortiWeb administrator deleted a certificate authorities (CA) group.

Table 120:

Field name	Description
ID (log_id)	00009011 See “Log ID numbers” on page 23.

Table 121:

Example
<pre>date=2014-04-10 time=17:06:31 log_id=00009011 msg_id=000000179549 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted certificate ca-group ca_g from GUI(172.22.6.66) "</pre>

Related

- [00009001](#)

00009101

Table 122:

Meaning
A FortiWeb administrator added an intermediate CA certificate.

Table 123:

Field name	Description
ID (log_id)	00009101 See “Log ID numbers” on page 23.

Table 124:

Example
<pre>date=2014-04-10 time=17:09:10 log_id=00009101 msg_id=000000179550 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added certificate intermediate-certificate Inter_Cert_1 from GUI(172.22.6.66) "</pre>

Related

- [00009111](#)

00009111

Table 125:

Meaning
A FortiWeb administrator deleted an intermediate CA certificate.

Table 126:

Field name	Description
ID (log_id)	00009111 See “Log ID numbers” on page 23.

Table 127:

Example
<pre>date=2014-04-10 time=17:09:14 log_id=00009111 msg_id=000000179551 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted certificate intermediate-certificate Inter_Cert_1 from GUI(172.22.6.66)"</pre>

Related

- [00009101](#)

00009201

Table 128:

Meaning
A FortiWeb administrator added an intermediate CA certificate group.

Table 129:

Field name	Description
ID (log_id)	00009201 See “Log ID numbers” on page 23.

Table 130:

Example
<pre>date=2014-04-10 time=17:10:42 log_id=00009201 msg_id=000000179552 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added certificate intermediate-certificate-group inter_g from GUI(172.22.6.66) "</pre>

Related

- [00009211](#)

00009211

Table 131:

Meaning
A FortiWeb administrator deleted an intermediate CA certificate group.

Table 132:

Field name	Description
ID (log_id)	00009211 See “Log ID numbers” on page 23.

Table 133:

Example
<pre>date=2014-04-10 time=17:10:46 log_id=00009211 msg_id=000000179553 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted certificate intermediate-certificate-group inter_g from GUI(172.22.6.66)"</pre>

Related

- [00009201](#)

Table 134:

Meaning
A FortiWeb administrator added a certificate revocation list (CRL) configuration.

Table 135:

Field name	Description
ID (log_id)	00009301 See “Log ID numbers” on page 23.

Table 136:

Example
<pre>date=2014-04-10 time=17:12:24 log_id=00009301 msg_id=000000179554 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added certificate crl CRL_4 from GUI(172.22.6.66) "</pre>

Related

- [00008801](#)
- [00008811](#)
- [00009311](#)
- [11006701](#)

Table 137:

Meaning
A FortiWeb administrator deleted a certificate revocation list (CRL) configuration.

Table 138:

Field name	Description
ID (log_id)	00009311 See “Log ID numbers” on page 23.

Table 139:

Example
<pre>date=2014-04-10 time=17:12:28 log_id=00009311 msg_id=000000179555 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted certificate crl CRL_4 from GUI(172.22.6.66)"</pre>

Related

- [00008801](#)
- [00008811](#)
- [00009301](#)
- [11006701](#)

00009401

Table 140:

Meaning
A FortiWeb administrator added a certificate verification rule.

Table 141:

Field name	Description
ID (log_id)	00009401 See “Log ID numbers” on page 23.

Table 142:

Example
<pre>date=2014-04-10 time=17:15:06 log_id=00009401 msg_id=000000179559 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added certificate verify CV from GUI(172.22.6.66) "</pre>

Related

- [00009402](#)
- [00009411](#)

Table 143:

Meaning
A FortiWeb administrator edited a certificate verification rule.

Table 144:

Field name	Description
ID (log_id)	00009402 See “Log ID numbers” on page 23 .

Table 145:

Example
<pre>date=2014-04-10 time=17:15:11 log_id=00009402 msg_id=000000179560 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed certificate verify CV from GUI(172.22.6.66) "</pre>

Related

- [00009401](#)
- [00009411](#)

00009411

Table 146:

Meaning
A FortiWeb administrator deleted a certificate verification rule.

Table 147:

Field name	Description
ID (log_id)	00009411 See “Log ID numbers” on page 23 .

Table 148:

Example
<pre>date=2014-04-10 time=17:15:14 log_id=00009411 msg_id=000000179561 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted certificate verify CV from GUI(172.22.6.66) "</pre>

Related

- [00009401](#)
- [00009402](#)

Table 149:

Meaning
A FortiWeb administrator added a Server Name Indication (SNI) configuration.

Table 150:

Field name	Description
ID (log_id)	00009501 See “Log ID numbers” on page 23.

Table 151:

Example
<pre>date=2014-09-03 time=11:16:33 log_id=00009501 msg_id=000000003148 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added certificate sni online_store from GUI(172.20.120.61) "</pre>

Related

- [00009502](#)
- [00009511](#)

Table 152:

Meaning
A FortiWeb administrator changed a Server Name Indication (SNI) configuration.

Table 153:

Field name	Description
ID (log_id)	00009502 See “Log ID numbers” on page 23.

Table 154:

Example
<pre>date=2014-09-03 time=11:16:33 log_id=00009501 msg_id=000000003148 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin changed certificate sni online_store from GUI(172.20.120.61) "</pre>

Related

- [00009501](#)
- [00009511](#)

00009511

Table 155:

Meaning
A FortiWeb administrator deleted a Server Name Indication (SNI) configuration.

Table 156:

Field name	Description
ID (log_id)	00009511 See “Log ID numbers” on page 23.

Table 157:

Example
<pre>date=2014-09-03 time=11:25:07 log_id=00009511 msg_id=000000003149 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted certificate sni online_store from GUI(172.20.120.61) "</pre>

Related

- [00009501](#)
- [00009502](#)

00009702

Table 158:

Meaning
A FortiWeb administrator changed system-wide FortiGuard Antivirus scan settings.

Table 159:

Field name	Description
ID (log_id)	00009702 See “Log ID numbers” on page 23.

Table 160:

Example
<pre>date=2014-04-10 time=16:31:09 log_id=00009702 msg_id=000000734627 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed system-antivirus from GUI(172.22.6.237)"</pre>

Table 161:

Meaning
A FortiWeb administrator added a locally-defined account for a web site end-user.

Table 162:

Field name	Description
ID (log_id)	00010001 See “Log ID numbers” on page 23.

Table 163:

Example
<pre>date=2013-10-08 time=10:01:51 log_id=00010001 msg_id=0000000000079 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added local-user user1 from GUI(172.20.120.47) "</pre>

Related

- [00010001](#)
- [00010002](#)
- [00010201](#)
- [00010401](#)
- [00010501](#)

Table 164:

Meaning
A FortiWeb administrator changed a locally defined account for a web site end-user.

Table 165:

Field name	Description
ID (log_id)	00010002 See “Log ID numbers” on page 23.

Table 166:

Example
<pre>date=2013-10-08 time=10:01:56 log_id=00010002 msg_id=0000000000080 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed local-user user1 from GUI(172.20.120.47) "</pre>

Related

- [00010001](#)
- [00010011](#)
- [00010501](#)

00010011

Table 167:

Meaning
A FortiWeb administrator deleted a locally-defined account for a web site end-user.

Table 168:

Field name	Description
ID (log_id)	00010011 See “Log ID numbers” on page 23.

Table 169:

Example
<pre>date=2013-10-08 time=10:01:59 log_id=00010011 msg_id=00000000000081 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted local-user user1 from GUI(172.20.120.47) "</pre>

Related

- [00010001](#)
- [00010002](#)

Table 170:

Meaning
A FortiWeb administrator added an LDAP query.

Table 171:

Field name	Description
ID (log_id)	00010201 See “Log ID numbers” on page 23.

Table 172:

Example
<pre>date=2013-10-09 time=15:44:16 log_id=00010201 msg_id=0000000000310 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added ldap-user ldap-query1 from GUI(172.20.120.47) "</pre>

Related

- [00010202](#)
- [00010211](#)
- [00010001](#)
- [00003401](#)

Table 173:

Meaning
A FortiWeb administrator changed an LDAP query.

Table 174:

Field name	Description
ID (log_id)	00010202 See “Log ID numbers” on page 23 .

Table 175:

Example
<pre>date=2013-10-09 time=15:44:23 log_id=00010202 msg_id=0000000000311 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed ldap-user ldap-query1 from GUI(172.20.120.47) "</pre>

Related

- [00010201](#)
- [00010211](#)
- [00010001](#)
- [00003401](#)

Table 176:

Meaning
A FortiWeb administrator deleted an LDAP query.

Table 177:

Field name	Description
ID (log_id)	00010211 See “Log ID numbers” on page 23.

Table 178:

Example
<pre>date=2013-10-09 time=15:44:32 log_id=00010211 msg_id=0000000000312 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted ldap-user ldap-query1 from GUI(172.20.120.47) "</pre>

Related

- [00010201](#)
- [00010202](#)
- [00010001](#)
- [00003401](#)

00010401

Table 179:

Meaning
A FortiWeb administrator created a RADIUS query.

Table 180:

Field name	Description
ID (log_id)	00010401 See “Log ID numbers” on page 23.

Table 181:

Example
<pre>date=2013-10-08 time=10:02:59 log_id=00010401 msg_id=00000000000082 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added radius-user radius-query1 from GUI(172.20.120.47) "</pre>

Related

- [00010402](#)
- [00010411](#)
- [00010001](#)
- [00003401](#)

Table 182:

Meaning
A FortiWeb administrator changed a RADIUS query.

Table 183:

Field name	Description
ID (log_id)	00010402 See “Log ID numbers” on page 23.

Table 184:

Example
<pre>date=2013-10-08 time=10:03:14 log_id=00010402 msg_id=00000000000083 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed radius-user radius-query1 from GUI(172.20.120.47) "</pre>

Related

- [00010401](#)
- [00010411](#)
- [00010001](#)
- [00003401](#)

00010411

Table 185:

Meaning
A FortiWeb administrator deleted a RADIUS query.

Table 186:

Field name	Description
ID (log_id)	00010411 See “Log ID numbers” on page 23.

Table 187:

Example
<pre>date=2013-10-08 time=10:03:24 log_id=00010411 msg_id=00000000000084 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted radius-user radius-query1 from GUI(172.20.120.47) "</pre>

Related

- [00010401](#)
- [00010402](#)
- [00010001](#)
- [00003401](#)

Table 188:

Meaning
A FortiWeb administrator added an NTLM query.

Table 189:

Field name	Description
ID (log_id)	00010501 See “Log ID numbers” on page 23.

Table 190:

Example
<pre>date=2013-10-08 time=10:03:34 log_id=00010501 msg_id=00000000000085 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added ntlm-user ntlm-query1 from GUI(172.20.120.47) "</pre>

Related

- [00010502](#)
- [00010511](#)
- [00010001](#)

Table 191:

Meaning
A FortiWeb administrator changed an NTLM query.

Table 192:

Field name	Description
ID (log_id)	00010502 See “Log ID numbers” on page 23.

Table 193:

Example
<pre>date=2013-10-08 time=10:03:44 log_id=00010502 msg_id=00000000000086 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed ntlm-user ntlm-query1 from GUI(172.20.120.47) "</pre>

Related

- [00010501](#)
- [00010511](#)
- [00010001](#)

Table 194:

Meaning
A FortiWeb administrator deleted an NTLM query.

Table 195:

Field name	Description
ID (log_id)	00010511 See “Log ID numbers” on page 23.

Table 196:

Example
<pre>date=2013-10-08 time=10:03:54 log_id=00010511 msg_id=00000000000087 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted ntlm-user ntlm-query1 from GUI(172.20.120.47) "</pre>

Related

- [00010501](#)
- [00010502](#)
- [00010001](#)

Table 197:

Meaning
A FortiWeb administrator added a user group.

Table 198:

Field name	Description
ID (log_id)	00010601 See “Log ID numbers” on page 23.

Table 199:

Example
<pre>date=2013-10-08 time=10:04:07 log_id=00010601 msg_id=00000000000082 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added User Group user-group1 from GUI(172.20.120.47) "</pre>

Related

- [00010602](#)
- [00010611](#)
- [00010201](#)
- [00010401](#)
- [00010501](#)
- [00010001](#)

Table 200:

Meaning
A FortiWeb administrator changed a user group.

Table 201:

Field name	Description
ID (log_id)	00010602 See “Log ID numbers” on page 23.

Table 202:

Example
<pre>date=2013-10-08 time=10:06:24 log_id=00010602 msg_id=00000000000083 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed user user-group user-group1 from GUI(172.20.120.47) "</pre>

Related

- [00010601](#)
- [00010611](#)
- [00010201](#)
- [00010401](#)
- [00010501](#)
- [00010001](#)

Table 203:

Meaning
A FortiWeb administrator deleted a user group.

Table 204:

Field name	Description
ID (log_id)	00010611 See “Log ID numbers” on page 23.

Table 205:

Example
<pre>date=2013-10-08 time=10:06:34 log_id=00010611 msg_id=00000000000084 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin deleted user user-group user-group1 from GUI(172.20.120.47) "</pre>

Related

- [00010602](#)
- [00010601](#)
- [00010201](#)
- [00010401](#)
- [00010501](#)
- [00010001](#)

Table 206:

Meaning
A FortiWeb administrator added an administrator group.

Table 207:

Field name	Description
ID (log_id)	00010701 See “Log ID numbers” on page 23.

Table 208:

Example
<pre>date=2013-10-08 time=10:06:46 log_id=00010701 msg_id=00000000000085 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added user admin-group admin-query-group1 from GUI(172.20.120.47) "</pre>

Related

- [00010711](#)
- [00010201](#)
- [00010401](#)
- [00003401](#)

00010711

Table 209:

Meaning
A FortiWeb administrator deleted an administrator group.

Table 210:

Field name	Description
ID (log_id)	00010711 See “Log ID numbers” on page 23.

Table 211:

Example
<pre>date=2013-10-08 time=10:06:46 log_id=00010701 msg_id=00000000000085 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin deleted user admin-group admin-query-group1 from GUI(172.20.120.47) "</pre>

Related

- [00010701](#)
- [00010201](#)
- [00010401](#)
- [00003401](#)

Table 212:

Meaning
<p>During a firmware upgrade, if the new firmware uses a different format for any existing settings, FortiWeb will attempt also to upgrade the configuration. If FortiWeb had to convert any settings to the new format, this log is recorded.</p> <p>Normally, no action is required. However, if you notice any behavior changes after the upgrade, you may want to compare your configuration with a backup copy to verify that it has been converted correctly. This is especially true if you have not followed the upgrade path recommended in the Release Notes.</p>

Table 213:

Field name	Description
ID (log_id)	00020088 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	information See “Priority level” on page 24.
User (user)	unknown
User Interface (ui)	
Action (action)	upgrade
Status (status)	success
Message (msg)	The old configurations are not compatible with the new version, and some of them have been changed to be correct.

Table 214:

Example
<pre>date=2012-11-04 time=19:11:01 log_id=00020088 msg_id=000000853622 type=event subtype="system" pri=information device_id=FVVM080000005545 vd="root" timezone="(GMT-8:00) Pacific Time (US&Canada)" user=unknown ui="" action=upgrade status=success reason=none msg="The old configurations are not compatible with the new version, and some of them have been changed to be correct."</pre>

Table 215:

Meaning
A FortiWeb administrator configured a connection to a Syslog server.

Table 216:

Field name	Description
ID (log_id)	00020201 See “Log ID numbers” on page 23 .

Table 217:

Example
<pre>date=2014-04-10 time=11:43:02 log_id=00020201 msg_id=000001014451 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added syslog-policy 1 from GUI(172.22.6.231) "</pre>

Related

- [00020202](#)
- [00020211](#)

Table 218:

Meaning
A FortiWeb administrator changed the configuration of a connection to a Syslog server.

Table 219:

Field name	Description
ID (log_id)	00020202 See “Log ID numbers” on page 23.

Table 220:

Example
<pre>date=2014-04-10 time=11:43:32 log_id=00020202 msg_id=000001014452 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed syslog-policy 1 from GUI(172.22.6.231) "</pre>

Related

- [00020201](#)
- [00020211](#)

Table 221:

Meaning
A FortiWeb administrator deleted a connection to a Syslog server.

Table 222:

Field name	Description
ID (log_id)	00020211 See “Log ID numbers” on page 23.

Table 223:

Example
<pre>date=2014-04-10 time=11:43:42 log_id=00020211 msg_id=000001014453 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted syslog-policy 1 from GUI(172.22.6.231) "</pre>

Related

- [00020201](#)
- [00020202](#)

Table 224:

Meaning
A FortiWeb administrator added an email policy.

Table 225:

Field name	Description
ID (log_id)	00020301 See “Log ID numbers” on page 23.

Table 226:

Example
<pre>date=2014-04-10 time=11:37:10 log_id=00020301 msg_id=000001014448 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added mail-policy test from GUI(172.22.6.231) "</pre>

Related

- [00020302](#)
- [00020311](#)

Table 227:

Meaning
A FortiWeb administrator made changes to an email policy.

Table 228:

Field name	Description
ID (log_id)	00020302 See “Log ID numbers” on page 23.

Table 229:

Example
<pre>date=2014-04-10 time=11:38:20 log_id=00020302 msg_id=000001014449 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed mail-policy test from GUI(172.22.6.231) "</pre>

Related

- [00020302](#)
- [00020311](#)

Table 230:

Meaning
A FortiWeb administrator deleted an email policy.

Table 231:

Field name	Description
ID (log_id)	00020311 See “Log ID numbers” on page 23.

Table 232:

Example
<pre>date=2014-04-10 time=11:40:17 log_id=00020311 msg_id=000001014450 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted mail-policy test from GUI(172.22.6.231) "</pre>

Related

- [00020302](#)
- [00020311](#)

Table 233:

Meaning
A FortiWeb administrator added a configuration that sends log messages to a remote FortiAnalyzer appliance.

Table 234:

Field name	Description
ID (log_id)	00020801 See “Log ID numbers” on page 23.

Table 235:

Example
<pre>date=2014-04-10 time=12:06:28 log_id=00020801 msg_id=000001014461 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added fortianalyzer-policy test from GUI(172.22.6.231) "</pre>

Related

- [00020802](#)
- [00020811](#)

Table 236:

Meaning
A FortiWeb administrator made changes to a configuration that sends log messages to a remote FortiAnalyzer appliance.

Table 237:

Field name	Description
ID (log_id)	00020802 See “Log ID numbers” on page 23.

Table 238:

Example
<pre>date=2014-04-10 time=12:07:10 log_id=00020802 msg_id=000001014462 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed fortianalyzer-policy test from GUI(172.22.6.231)"</pre>

Related

- [00020801](#)
- [00020811](#)

00020811

Table 239:

Meaning
A FortiWeb administrator deleted a configuration that sends log messages to a remote FortiAnalyzer appliance.

Table 240:

Field name	Description
ID (log_id)	00020811 See “Log ID numbers” on page 23.

Table 241:

Example
<pre>date=2014-04-10 time=12:07:40 log_id=00020811 msg_id=000001014463 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted fortianalyzer-policy test from GUI(172.22.6.231) "</pre>

Related

- [00020801](#)
- [00020802](#)

Table 242:

Meaning
A FortiWeb administrator added a trigger policy that is used by the notification process.

Table 243:

Field name	Description
ID (log_id)	00020901 See “Log ID numbers” on page 23.

Table 244:

Example
<pre>date=2014-04-10 time=12:08:51 log_id=00020901 msg_id=000001014464 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added trigger-policy 1 from GUI(172.22.6.231) "</pre>

Related

- [00020902](#)
- [00020911](#)

Table 245:

Meaning
A FortiWeb administrator made a change to a trigger policy that is used by the notification process.

Table 246:

Field name	Description
ID (log_id)	00020902 See “Log ID numbers” on page 23.

Table 247:

Example
<pre>date=2014-04-10 time=12:09:39 log_id=00020902 msg_id=000001014465 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed trigger-policy 1 from GUI(172.22.6.231) "</pre>

Related

- [00020901](#)
- [00020911](#)

Table 248:

Meaning
A FortiWeb administrator deleted a trigger policy that is used by the notification process.

Table 249:

Field name	Description
ID (log_id)	00020911 See “Log ID numbers” on page 23.

Table 250:

Example
<pre>date=2014-04-10 time=12:10:10 log_id=00020911 msg_id=000001014466 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted trigger-policy 1 from GUI(172.22.6.231) "</pre>

Related

- [00020901](#)
- [00020902](#)

Table 251:

Meaning
A FortiWeb administrator enabled or disabled storing logs on the appliance's hard disk.

Table 252:

Field name	Description
ID (log_id)	00021002 See "Log ID numbers" on page 23.

Table 253:

Example
<pre>date=2013-10-08 time=01:34:07 log_id=00021002 msg_id=0000000000016 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed setting for saving logs to disk from GUI"</pre>

Related

- [00021302](#)

Table 254:

Meaning
A FortiWeb administrator changed the configuration for event logging to memory (RAM).

Table 255:

Field name	Description
ID (log_id)	00021102 See “Log ID numbers” on page 23.

Table 256:

Example
<pre>date=2014-04-10 time=12:10:52 log_id=00021102 msg_id=000001014467 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed memory from GUI(172.22.6.231) "</pre>

00021140

Table 257:

Meaning
The FortiWeb's system clock was updated via NTP. If you are using FortiWeb-VM, this message is often displayed after you unsuspend the VM.

Table 258:

Field name	Description
ID (log_id)	00021140 See "Log ID numbers" on page 23.
Level (pri)	notification See "Priority level" on page 24.
User (user)	ntp_daemon
User Interface (ui)	none

Table 259:

Example
<pre>date=2014-09-11 time=11:51:56 log_id=00021140 msg_id=000000133596 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=notice trigger_policy="" user=ntp_daemon ui=none action=edit status=success msg="global time setting change field:date-time The ntp daemon changed time from Wed Sep 10 20:51:48 2014 to Thu Sep 11 03:51:56 2014 "</pre>

Related

- [00001002](#)

00021202

Table 260:

Meaning
A FortiWeb administrator changed the configuration for recording attack log messages on the local FortiWeb disk.

Table 261:

Field name	Description
ID (log_id)	00021202 See “Log ID numbers” on page 23.

Table 262:

Example
<pre>date=2014-04-10 time=12:02:33 log_id=00021202 msg_id=000001014457 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed attack-log from GUI(172.22.6.231) "</pre>

Table 263:

Meaning
A FortiWeb administrator enabled or disabled storing traffic logs on the appliance's hard disk.

Table 264:

Field name	Description
ID (log_id)	00021302 See "Log ID numbers" on page 23.

Table 265:

Example
<pre>date=2013-10-08 time=01:34:51 log_id=00021302 msg_id=0000000000017 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=edit status=success msg="User admin changed traffic log setting from GUI"</pre>

Related

- [00021002](#)

Table 266:

Meaning
A FortiWeb administrator made changes to the configuration for event log recording.

Table 267:

Field name	Description
ID (log_id)	00021402 See “Log ID numbers” on page 23.

Table 268:

Example
<pre>date=2014-04-10 time=17:48:20 log_id=00021402 msg_id=000001015952 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed event-log from GUI(172.22.6.231) "</pre>

Table 269:

Meaning
FortiWeb does not have enough hard disk space in order to store data gathered for auto-learning.
Solution
<p>If you have just updated the firmware, check the Release Notes. (Some firmware updates require that you resize the partitions before you upgrade. If you missed this step, it will cause this log message.)</p> <p>If this log message is preceded by log ID 11006005, auto-learning data could not be stored because the data disk's file system is not currently mounted. For solutions, see 11006005.</p> <p>Otherwise, delete any unnecessary auto-learning data, and disable it in policies where it is no longer required. This will free disk space.</p>

Table 270:

Field name	Description
ID (log_id)	00022997 See "Log ID numbers" on page 23.
Sub Type (subtype)	system See "Subtypes" on page 24.
Level (pri)	alert See "Priority level" on page 24.
Message (msg)	Disk free space is not enough for autolearn

Table 271:

Example
<pre>date=2012-09-27 time=07:44:00 log_id=00022997 msg_id=0000000018352 type=event subtype="system" pri=alert device_id=FV-1KC3R11700136 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" msg="Disk free space is not enough for autolearn"</pre>

Related

- [11006005](#)

00030001

Table 272:

Meaning
An administrator created an IP-layer static route.

Table 273:

Field name	Description
ID (log_id)	00030001 See “Log ID numbers” on page 23.

Table 274:

Example
<pre>date=2013-10-06 time=11:03:37 log_id=00030001 msg_id=000000001086 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=add status=success msg="User admin added static-route 1 from console"</pre>

Related

- [00004402](#)
- [00006202](#)
- [00030002](#)
- [00030011](#)
- [00040623](#)

Table 275:

Meaning
An administrator changed an IP-layer static route.

Table 276:

Field name	Description
ID (log_id)	00030002 See “Log ID numbers” on page 23.

Table 277:

Example
<pre>date=2013-10-06 time=11:03:47 log_id=00030002 msg_id=0000000001087 device_id=FVVM0400000010871 vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=add status=success msg="User admin changed static-route 1 from console"</pre>

Related

- [00004402](#)
- [00006202](#)
- [00030001](#)
- [00030011](#)
- [00040623](#)

Table 278:

Meaning
An administrator deleted an IP-layer static route.

Table 279:

Field name	Description
ID (log_id)	00030011 See “Log ID numbers” on page 23.

Table 280:

Example
<pre>date=2013-10-06 time=11:00:12 log_id=00030011 msg_id=000000001084 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=del status=success msg="User admin deleted static-route 1 from console"</pre>

Related

- [00030001](#)
- [00030002](#)
- [00004402](#)
- [00040623](#)

Table 281:

Meaning
<p>Either:</p> <ul style="list-style-type: none"> The maximum number of concurrent sessions has been reached. For more information on model- or configuration-dependent limits, see the FortiWeb Administration Guide. A policy was reloaded after a configuration change in order to free memory.

Table 282:

Field name	Description
ID (log_id)	00032006 See “Log ID numbers” on page 23 .
Sub Type (subtype)	admin See “Subtypes” on page 24 .
Level (pri)	information (login or daemon start) or alert (concurrent session limit reached) See “Priority level” on page 24 .
Message (msg)	
	policy <policy_name> concurrent session exceed threshold
	policy <policy_name> refreshed to free resources

Table 283:

Example
<pre>date=2012-10-25 time=09:31:07 log_id=00032006 msg_id=000066877877 type=event subtype="admin" pri=alert device_id=FVVM020000003619 vd="root" timezone="(GMT)Greenwich Mean Time: Dublin,Edinburgh,Lisbon,London" msg="policy policy1 concurrent session exceed threshold"</pre>
<pre>date=2013-01-16 time=12:27:33 log_id=00032006 msg_id=000000201047 type=event subtype="admin" pri=information device_id=FVVM020000003619 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" msg="policy policy1 refreshed to free resources"</pre>

Related

- [10000014](#)

00040001

Table 284:

Meaning
An administrator created a server availability monitor ("health check").

Table 285:

Field name	Description
ID (log_id)	00040001 See "Log ID numbers" on page 23.

Table 286:

Example
<pre>date=2013-10-08 time=10:14:10 log_id=00040001 msg_id=0000000000105 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added health uptime-check1 from GUI(172.20.120.47) "</pre>

Related

- [00040002](#)
- [00040011](#)
- [19999496](#)

Table 287:

Meaning
An administrator changed a server availability monitor ("health check").

Table 288:

Field name	Description
ID (log_id)	00040002 See "Log ID numbers" on page 23.

Table 289:

Example
<pre>date=2013-10-08 time=10:14:20 log_id=00040002 msg_id=0000000000106 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed health uptime-check1 from GUI(172.20.120.47) "</pre>

Related

- [00040001](#)
- [00040011](#)
- [19999496](#)

Table 290:

Meaning
An administrator deleted a server availability monitor ("health check").

Table 291:

Field name	Description
ID (log_id)	00040011 See "Log ID numbers" on page 23.

Table 292:

Example
date=2013-10-08 time=10:14:30 log_id=00040011 msg_id=0000000000107 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted health uptime-check1 from GUI(172.20.120.47) "

Related

- [00040002](#)
- [00040001](#)
- [19999496](#)

Table 293:

Meaning
An administrator created a network service definition such as HTTP_8080 or HTTPS4443.

Table 294:

Field name	Description
ID (log_id)	00040301 See “Log ID numbers” on page 23.

Table 295:

Example
<pre>date=2013-10-08 time=10:23:14 log_id=00040301 msg_id=000000000138 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=succes smsg="User admin added custome service soap-service from GUI(172.20.120.47) "</pre>

Related

- [00040302](#)
- [00040311](#)

Table 296:

Meaning
An administrator changed a network service definition.

Table 297:

Field name	Description
ID (log_id)	00040302 See “Log ID numbers” on page 23.

Table 298:

Example
<pre>date=2013-10-08 time=10:23:18 log_id=00040302 msg_id=0000000000139 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=succes smsg="User admin changed custom service soap-service from GUI(172.20.120.47) "</pre>

Related

- [00040301](#)
- [00040311](#)

Table 299:

Meaning
An administrator deleted a network service definition.

Table 300:

Field name	Description
ID (log_id)	00040311 See “Log ID numbers” on page 23.

Table 301:

Example
<pre>date=2013-10-08 time=10:23:34 log_id=00040311 msg_id=0000000000140 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=succes smsg="User admin deleted custom service soap-service from GUI(172.20.120.47) "</pre>

Related

- [00040302](#)
- [00040301](#)

00040501

Table 302:

Meaning
An administrator added a virtual server.

Table 303:

Field name	Description
ID (log_id)	00040501 See “Log ID numbers” on page 23.

Table 304:

Example
<pre>date=2014-04-10 time=14:15:55 log_id=00040501 msg_id=000000055147 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added Virtual Server 1 from GUI(172.22.6.149) "</pre>

Related

- [00040502](#)
- [00040511](#)

Table 305:

Meaning
An administrator edited a virtual server.

Table 306:

Field name	Description
ID (log_id)	00040502 See “Log ID numbers” on page 23.

Table 307:

Example
<pre>date=2014-04-10 time=14:16:22 log_id=00040502 msg_id=000000055149 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed Virtual Server FWB_Vserver from GUI(172.22.6.149) "</pre>

Related

- [00040501](#)
- [00040511](#)

Table 308:

Meaning
An administrator deleted a virtual server.

Table 309:

Field name	Description
ID (log_id)	00040511 See “Log ID numbers” on page 23.

Table 310:

Example
<pre>date=2014-04-10 time=14:16:11 log_id=00040511 msg_id=000000055148 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted Virtual Server 1 from GUI(172.22.6.149) "</pre>

Related

- [00040501](#)
- [00040502](#)

Table 311:

Meaning
An administrator created an HTTP-layer route ("content route").

Table 312:

Field name	Description
ID (log_id)	00040601 See "Log ID numbers" on page 23.

Table 313:

Example
<pre>date=2013-10-08 time=10:11:09 log_id=00040601 msg_id=00000000000091 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added server-policy http-content-routing content-route1 from GUI(172.20.120.47) "</pre>

Related

- [00040611](#)
- [00040623](#)
- [00030001](#)

Table 314:

Meaning
An administrator deleted an HTTP-layer route ("content route").

Table 315:

Field name	Description
ID (log_id)	00040611 See "Log ID numbers" on page 23.

Table 316:

Example
<pre>date=2013-10-08 time=10:11:45 log_id=00040611 msg_id=0000000000093 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted server-policy http-content-routing content-route1 from GUI(172.20.120.47) "</pre>

Related

- [00040601](#)
- [00040623](#)
- [00030001](#)

Table 317:

Meaning
An administrator changed an HTTP-layer route ("content route").

Table 318:

Field name	Description
ID (log_id)	00040623 See "Log ID numbers" on page 23.

Table 319:

Example
<pre>date=2014-04-10 time=14:24:08 log_id=00040623 msg_id=000000055157 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=notice trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin changed server-policy http-content-routing FWB_ContentRouting1 list 2 from GUI(172.22.6.149) "</pre>

Related

- [00040601](#)
- [00040611](#)
- [00030001](#)

Table 320:

Meaning
An administrator uploaded a customized HTTP error web page.

Table 321:

Field name	Description
ID (log_id)	00040751 See “Log ID numbers” on page 23.

Table 322:

Example
<pre>date=2014-04-10 time=17:18:58 log_id=00040751 msg_id=000000820249 device_id=FVVM020000018475 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added server-policy error-page myerrorpage from GUI(172.22.6.230)</pre>

Related

- [00040752](#)
- [00040761](#)

Table 323:

Meaning
An administrator changed the description for a customized HTTP error web page.

Table 324:

Field name	Description
ID (log_id)	00040752 See “Log ID numbers” on page 23.

Table 325:

Example
date=2013-10-08 time=10:22:11 log_id=00040752 msg_id=000000000132 device_id=FVVM00UNLICENSED timezone="(GMT-5:00) Eastern Time (US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed server-policy error-page custom-500 from GUI(172.20.120.47) "

Related

- [00040751](#)
- [00040761](#)

Table 326:

Meaning
An administrator deleted a customized HTTP error web page.

Table 327:

Field name	Description
ID (log_id)	00040761 See “Log ID numbers” on page 23.

Table 328:

Example
<pre>date=2013-10-08 time=10:22:21 log_id=00040761 msg_id=000000000133 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted server-policy error-page custom-500 from GUI(172.20.120.47) "</pre>

Related

- [00040751](#)
- [00040752](#)

Table 329:

Meaning
An administrator created a customized data type definition.

Table 330:

Field name	Description
ID (log_id)	00040801 See “Log ID numbers” on page 23.

Table 331:

Example
<pre>date=2013-10-08 time=10:36:11 log_id=00040801 msg_id=000000000156 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added server-policy pattern custom-data-type data-type1 from GUI(172.20.120.47) "</pre>

Related

- [00040802](#)
- [00040811](#)

Table 332:

Meaning
An administrator changed a customized data type definition.

Table 333:

Field name	Description
ID (log_id)	00040802 See “Log ID numbers” on page 23.

Table 334:

Example
<pre>date=2013-10-08 time=10:36:14 log_id=00040802 msg_id=0000000000157 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed server-policy pattern custom-data-type data-type1 from GUI(172.20.120.47) "</pre>

Related

- [00040801](#)
- [00040811](#)

Table 335:

Meaning
An administrator deleted a customized data type definition.

Table 336:

Field name	Description
ID (log_id)	00040811 See “Log ID numbers” on page 23.

Table 337:

Example
<pre>date=2013-10-08 time=10:36:21 log_id=00040811 msg_id=000000000158 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted server-policy pattern custom-data-type data-type1 from GUI(172.20.120.47) "</pre>

Related

- [00040802](#)
- [00040801](#)

Table 338:

Meaning
An administrator created a group of customized data type definitions.

Table 339:

Field name	Description
ID (log_id)	00040901 See “Log ID numbers” on page 23.

Table 340:

Example
<pre>date=2013-10-08 time=10:37:29 log_id=00040901 msg_id=0000000000160 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added server-policy pattern data-type-group custom-data-type-group1 from GUI(172.20.120.47) "</pre>

Related

- [00040902](#)
- [00040911](#)

Table 341:

Meaning
An administrator changed a group of customized data type definitions.

Table 342:

Field name	Description
ID (log_id)	00040902 See “Log ID numbers” on page 23.

Table 343:

Example
<pre>date=2013-10-08 time=10:37:39 log_id=00040902 msg_id=0000000000161 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed server-policy pattern data-type-group custom-data-type-group1 from GUI(172.20.120.47) "</pre>

Related

- [00040901](#)
- [00040911](#)

Table 344:

Meaning
An administrator deleted a group of customized data type definitions.

Table 345:

Field name	Description
ID (log_id)	00040911 See “Log ID numbers” on page 23.

Table 346:

Example
<pre>date=2013-10-08 time=10:37:49 log_id=00040911 msg_id=0000000000161 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted server-policy pattern data-type-group custom-data-type-group1 from GUI(172.20.120.47) "</pre>

Related

- [00040902](#)
- [00040901](#)

Table 347:

Meaning
An administrator created a customized suspicious URL definition.

Table 348:

Field name	Description
ID (log_id)	00041001 See “Log ID numbers” on page 23.

Table 349:

Example
<pre>date=2013-10-08 time=10:35:29 log_id=00041001 msg_id=0000000000152 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-susp-url suspicious-url1 from GUI(172.20.120.47) "</pre>

Related

- [00041002](#)
- [00041011](#)

Table 350:

Meaning
An administrator changed a customized suspicious URL definition.

Table 351:

Field name	Description
ID (log_id)	00041002 See “Log ID numbers” on page 23.

Table 352:

Example
<pre>date=2013-10-08 time=10:35:39 log_id=00041002 msg_id=0000000000153 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-susp-url suspicious-url1 from GUI(172.20.120.47) "</pre>

Related

- [00041011](#)
- [00041001](#)

00041011

Table 353:

Meaning
An administrator deleted a customized suspicious URL definition.

Table 354:

Field name	Description
ID (log_id)	00041011 See “Log ID numbers” on page 23.

Table 355:

Example
<pre>date=2013-10-08 time=10:35:49 log_id=00041011 msg_id=0000000000153 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted custom-susp-url suspicious-url1 from GUI(172.20.120.47) "</pre>

Related

- [00041002](#)
- [00041001](#)

Table 356:

Meaning
An administrator created a group of customized suspicious URL definitions ("policy").

Table 357:

Field name	Description
ID (log_id)	00041101 See "Log ID numbers" on page 23.

Table 358:

Example
<pre>date=2013-10-08 time=10:35:44 log_id=00041101 msg_id=0000000000153 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada) "type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-susp-url-rule suspicious-urls-all from GUI(172.20.120.47) "</pre>

Related

- [00041102](#)
- [00041111](#)

Table 359:

Meaning
An administrator changed a group of customized suspicious URL definitions.

Table 360:

Field name	Description
ID (log_id)	00041102 See “Log ID numbers” on page 23.

Table 361:

Example
<pre>date=2013-10-08 time=10:35:45 log_id=00041102 msg_id=0000000000154 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada) "type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-susp-url-rule suspicious-urls-all from GUI(172.20.120.47) "</pre>

Related

- [00041101](#)
- [00041111](#)

00041111

Table 362:

Meaning
An administrator deleted a group of customized suspicious URL definitions.

Table 363:

Field name	Description
ID (log_id)	00041111 See “Log ID numbers” on page 23.

Table 364:

Example
<pre>date=2013-10-08 time=10:35:49 log_id=00041111 msg_id=0000000000153 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted custom-susp-url suspicious-url1 from GUI(172.20.120.47) "</pre>

Related

- [00041101](#)
- [00041102](#)

00041201

Table 365:

Meaning
An administrator created a customized suspicious URL definition ("rule").

Table 366:

Field name	Description
ID (log_id)	00041201 See "Log ID numbers" on page 23.

Table 367:

Example
<pre>date=2013-10-08 time=10:36:50 log_id=00041201 msg_id=0000000000157 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added server-policy pattern suspicious-url-rule custom-suspicious-urls from GUI(172.20.120.47) "</pre>

Related

- [00041202](#)
- [00041211](#)

Table 368:

Meaning
An administrator changed a customized suspicious URL definition.

Table 369:

Field name	Description
ID (log_id)	00041202 See “Log ID numbers” on page 23.

Table 370:

Example
<pre>date=2013-10-08 time=10:36:50 log_id=00041202 msg_id=0000000000158 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed server-policy pattern suspicious-url-rule custom-suspicious-urls from GUI(172.20.120.47) "</pre>

Related

- [00041201](#)
- [00041211](#)

00041211

Table 371:

Meaning
An administrator deleted a customized suspicious URL definition.

Table 372:

Field name	Description
ID (log_id)	00041211 See “Log ID numbers” on page 23.

Table 373:

Example
<pre>date=2013-10-08 time=10:36:50 log_id=00041211 msg_id=000000000158 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted server-policy pattern suspicious-url-rule custom-suspicious-urls from GUI(172.20.120.47) "</pre>

Related

- [00041201](#)
- [00041202](#)

Table 374:

Meaning
<p>An administrator disabled or enabled either:</p> <ul style="list-style-type: none"> • a predefined global white list object or • a definition of a known search engine crawler.

Table 375:

Field name	Description
ID (log_id)	<p>00041302</p> <p>See “Log ID numbers” on page 23.</p>

Table 376:

Examples
<pre>date=2014-01-08 time=17:39:20 log_id=00041302 msg_id=000000004887 device_id=FV-3KC3R09700002 vd="adom_auto" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=notice trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed the Global White List"</pre>
<pre>date=2013-10-08 time=10:22:50 log_id=00041302 msg_id=000000000136 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=notification trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed the Global known Engines"</pre>

00041401

Table 377:

Meaning
An administrator created an allowed/protected Host : definition.

Table 378:

Field name	Description
ID (log_id)	00041401 See “Log ID numbers” on page 23.

Table 379:

Example
<pre>date=2013-10-08 time=10:12:46 log_id=00041401 msg_id=0000000000101 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added Protected Hostnames example_co_jp from GUI(172.20.120.47) "</pre>

Related

- [00041402](#)
- [00041411](#)

Table 380:

Meaning
An administrator changed an allowed/protected Host : definition.

Table 381:

Field name	Description
ID (log_id)	00041402 See “Log ID numbers” on page 23.

Table 382:

Example
<pre>date=2013-10-08 time=10:12:52 log_id=00041402 msg_id=0000000000102 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed Protected Hostnames example_com from GUI(172.20.120.47) "</pre>

Related

- [00041401](#)
- [00041411](#)

00041411

Table 383:

Meaning
An administrator deleted an allowed/protected Host : definition.

Table 384:

Field name	Description
ID (log_id)	00041411 See “Log ID numbers” on page 23.

Table 385:

Example
<pre>date=2013-10-15 time=20:01:30 log_id=00041411 msg_id=0000000000637 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted Protected Hostnames example_co_uk from GUI(192.168.1.28) "</pre>

Related

- [00041401](#)
- [00041402](#)

Table 386:

Meaning
An administrator created an interpreter to locate parameters in a dynamic URL ("URL replacer") when using auto-learning.

Table 387:

Field name	Description
ID (log_id)	00041601 See "Log ID numbers" on page 23.

Table 388:

Example
date=2013-10-08 time=10:34:46 log_id=00041601 msg_id=000000000148 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added server-policy custom-application url-replace url-interpreter1 from GUI(172.20.120.47) "

Related

- [00041602](#)
- [00041611](#)

Table 389:

Meaning
An administrator changed a URL replacer.

Table 390:

Field name	Description
ID (log_id)	00041602 See “Log ID numbers” on page 23.

Table 391:

Example
<pre>date=2013-10-15 time=20:31:58 log_id=00041602 msg_id=0000000000645 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed server-policy custom-application url-replace url-interpretel from GUI(192.168.1.28) "</pre>

Related

- [00041601](#)
- [00041611](#)

00041611

Table 392:

Meaning
An administrator deleted a URL replacer.

Table 393:

Field name	Description
ID (log_id)	00041611 See “Log ID numbers” on page 23.

Table 394:

Example
<pre>date=2013-10-08 time=10:33:21 log_id=00041611 msg_id=000000000147 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted server-policy custom-application url-replace url-interpreter1 from GUI(172.20.120.47) "</pre>

Related

- [00041601](#)
- [00041602](#)

Table 395:

Meaning
An administrator created a group of URL replacers ("application policy").

Table 396:

Field name	Description
ID (log_id)	00041801 See "Log ID numbers" on page 23.

Table 397:

Example
<pre>date=2013-10-15 time=20:32:24 log_id=00041801 msg_id=0000000000647 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added server-policy custom-application application-policy url-interpreter-group1 from GUI(192.168.1.28) "</pre>

Related

- [00041802](#)
- [00041811](#)

Table 398:

Meaning
An administrator changed a group of URL replacers ("application policy").

Table 399:

Field name	Description
ID (log_id)	00041802 See "Log ID numbers" on page 23.

Table 400:

Example
<pre>date=2013-10-15 time=20:32:29 log_id=00041802 msg_id=0000000000648 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed server-policy custom-application application-policy url-interpreter-group1 from GUI(192.168.1.28) "</pre>

Related

- [00041801](#)
- [00041811](#)

Table 401:

Meaning
An administrator deleted a group of URL replacers ("application policy").

Table 402:

Field name	Description
ID (log_id)	00041811 See "Log ID numbers" on page 23.

Table 403:

Example
<pre>date=2013-10-15 time=20:32:39 log_id=00041811 msg_id=0000000000649 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted server-policy custom-application application-policy url-interpreter-group1 from GUI(192.168.1.28) "</pre>

Related

- [00041801](#)
- [00041802](#)

Table 404:

Meaning
An administrator created a server policy.

Table 405:

Field name	Description
ID (log_id)	00043001 See “Log ID numbers” on page 23.

Table 406:

Example
<pre>date=2013-10-08 time=10:20:37 log_id=00043001 msg_id=0000000000128 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added policy policy2 from GUI(172.20.120.47) "</pre>

Related

- [00043011](#)
- [00043002](#)

Table 407:

Meaning
An administrator changed a server policy.

Table 408:

Field name	Description
ID (log_id)	00043002 See “Log ID numbers” on page 23.

Table 409:

Example
<pre>date=2013-10-08 time=10:20:04 log_id=00043002 msg_id=000000000125 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed policy policy1 from GUI(172.20.120.47) "</pre>

Related

- [00043001](#)
- [00043011](#)

Table 410:

Meaning
An administrator deleted a server policy.

Table 411:

Field name	Description
ID (log_id)	00043011 See “Log ID numbers” on page 23.

Table 412:

Example
<pre>date=2013-10-08 time=10:20:49 log_id=00043011 msg_id=0000000000130 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted policy policy2 from GUI(172.20.120.47) "</pre>

Related

- [00043001](#)
- [00043002](#)

Table 413:

Meaning
An administrator added a site publishing policy rule.

Table 414:

Field name	Description
ID (log_id)	00044001 See “Log ID numbers” on page 23.

Table 415:

Example
<pre>date=2014-04-10 time=16:24:11 log_id=00044001 msg_id=000000179495 device_id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added site-published-helper autotest.fwb.com from GUI(172.22.6.66) "</pre>

Related

- [00044002](#)
- [00044011](#)
- [00044401](#)
- [00044411](#)

Table 416:

Meaning
An administrator edited a site publishing policy rule.

Table 417:

Field name	Description
ID (log_id)	00044002 See “Log ID numbers” on page 23.

Table 418:

Example
<pre>date=2014-04-10 time=16:30:16 log_id=00044002 msg_id=0000000179501 device_id=FVVM0400000018473 vd="domain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed site-published-helper autotest1.fwb.com from GUI(172.22.6.66) "</pre>

Related

- [00044001](#)
- [00044011](#)
- [00044401](#)
- [00044411](#)

Table 419:

Meaning
An administrator deleted a site publishing policy rule.

Table 420:

Field name	Description
ID (log_id)	00044011 See “Log ID numbers” on page 23.

Table 421:

Example
<pre>date=2014-04-10 time=16:31:41 log_id=00044011 msg_id=000000179502 device_id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted site-published-helper autotest1.fwb.com from GUI(172.22.6.66) "</pre>

Related

- [00044001](#)
- [00044002](#)
- [00044401](#)
- [00044411](#)

00044401

Table 422:

Meaning
An administrator added a site publishing policy.

Table 423:

Field name	Description
ID (log_id)	00044401 See “Log ID numbers” on page 23.

Table 424:

Example
<pre>date=2014-04-10 time=16:32:28 log_id=00044401 msg_id=000000179503 device_id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added site-published-helper-policy dd from GUI(172.22.6.66) "</pre>

Related

- [00044411](#)
- [00044001](#)
- [00044002](#)
- [00044011](#)

00044411

Table 425:

Meaning
An administrator deleted a site publishing policy.

Table 426:

Field name	Description
ID (log_id)	00044411 See “Log ID numbers” on page 23.

Table 427:

Example
<pre>date=2014-04-10 time=16:38:07 log_id=00044411 msg_id=000000179507 device_id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted site-published-helper-policy dd from GUI(172.22.6.66) "</pre>

Related

- [00044401](#)
- [00044001](#)
- [00044002](#)
- [00044011](#)

Table 428:

Meaning
An administrator added a custom global whitelist item.

Table 429:

Field name	Description
ID (log_id)	00044501 See “Log ID numbers” on page 23.

Table 430:

Example
<pre>date=2014-04-10 time=15:03:01 log_id=00044501 msg_id=000000055170 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-global-whilte-list-group 1 from GUI(172.22.6.149) "</pre>

Related

- [00044502](#)
- [00044511](#)

Table 431:

Meaning
An administrator edited a custom global whitelist item.

Table 432:

Field name	Description
ID (log_id)	00044502 See “Log ID numbers” on page 23.

Table 433:

Example
<pre>date=2014-04-10 time=15:03:26 log_id=00044502 msg_id=000000055171 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-global-whilte-list-group 1 from GUI(172.22.6.149) "</pre>

Related

- [00044501](#)
- [00044511](#)

00044511

Table 434:

Meaning
An administrator deleted a custom global whitelist item.

Table 435:

Field name	Description
ID (log_id)	00044511 See “Log ID numbers” on page 23.

Table 436:

Example
<pre>date=2014-04-10 time=15:03:40 log_id=00044511 msg_id=000000055172 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted custom-global-whilte-list-group 1 from GUI(172.22.6.149) "</pre>

Related

- [00044501](#)
- [00044502](#)

Table 437:

Meaning
An administrator created a session persistence configuration.

Table 438:

Field name	Description
ID (log_id)	00046001 See “Log ID numbers” on page 23.

Table 439:

Example
<pre>date=2014-09-03 time=10:47:27 log_id=00046001 msg_id=000000003145 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added persistence-policy persistent_ip from GUI(172.20.120.61) "</pre>

Related

- [00046002](#)
- [00046011](#)

Table 440:

Meaning
An administrator edited a session persistence configuration.

Table 441:

Field name	Description
ID (log_id)	00046002 See “Log ID numbers” on page 23.

Table 442:

Example
<pre>date=2014-09-03 time=10:56:36 log_id=00046002 msg_id=000000003146 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed persistence-policy persistent_ip from GUI(172.20.120.61) "</pre>

Related

- [00046001](#)
- [00046011](#)

Table 443:

Meaning
An administrator deleted a session persistence configuration.

Table 444:

Field name	Description
ID (log_id)	00046011 See “Log ID numbers” on page 23.

Table 445:

Example
<pre>date=2014-09-03 time=10:56:56 log_id=00046011 msg_id=000000003147 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted persistence-policy persistent_ip from GUI(172.20.120.61) "</pre>

Related

- [00046001](#)
- [00046002](#)

00050001

Table 446:

Meaning
An administrator created a compression exemption.

Table 447:

Field name	Description
ID (log_id)	00050001 See “Log ID numbers” on page 23.

Table 448:

Example
<pre>date=2013-10-08 time=10:55:44 log_id=00050001 msg_id=0000000000240 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added exclude-url gzip-exempt1 from GUI(172.20.120.47) "</pre>

Related

- [00050002](#)
- [00050011](#)

Table 449:

Meaning
An administrator changed a compression exemption.

Table 450:

Field name	Description
ID (log_id)	00050002 See “Log ID numbers” on page 23.

Table 451:

Example
<pre>date=2013-10-08 time=10:55:55 log_id=00050002 msg_id=0000000000241 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed exclude-url gzip-exempt1 from GUI(172.20.120.47) "</pre>

Related

- [00050001](#)
- [00050011](#)

00050011

Table 452:

Meaning
An administrator deleted a compression exemption.

Table 453:

Field name	Description
ID (log_id)	00050011 See “Log ID numbers” on page 23.

Table 454:

Example
<pre>date=2013-10-08 time=10:56:55 log_id=00050011 msg_id=0000000000242 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted exclude-url gzip-exempt1 from GUI(172.20.120.47) "</pre>

Related

- [00050001](#)
- [00050002](#)

00050201

Table 455:

Meaning
An administrator created a decompressor.

Table 456:

Field name	Description
ID (log_id)	00050201 See “Log ID numbers” on page 23.

Table 457:

Example
<pre>date=2013-10-08 time=10:56:11 log_id=00050201 msg_id=0000000000243 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added file-uncompress-rule decompressor1 from GUI(172.20.120.47) "</pre>

Related

- [00050202](#)
- [00050211](#)

Table 458:

Meaning
An administrator changed a decompressor.

Table 459:

Field name	Description
ID (log_id)	00050202 See “Log ID numbers” on page 23.

Table 460:

Example
<pre>date=2013-10-08 time=10:56:23 log_id=00050202 msg_id=0000000000244 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed file-uncompress-rule decompressor1 from GUI(172.20.120.47) "</pre>

Related

- [00050201](#)
- [00050211](#)

Table 461:

Meaning
An administrator deleted a decompressor.

Table 462:

Field name	Description
ID (log_id)	00050211 See “Log ID numbers” on page 23.

Table 463:

Example
<pre>date=2013-10-08 time=10:56:43 log_id=00050211 msg_id=0000000000245 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin dleted file-uncompress-rule decompressor1 from GUI(172.20.120.47) "</pre>

Related

- [00050201](#)
- [00050202](#)

Table 464:

Meaning
An administrator created a compressor.

Table 465:

Field name	Description
ID (log_id)	00050401 See “Log ID numbers” on page 23.

Table 466:

Example
<pre>date=2013-10-08 time=10:56:34 log_id=00050401 msg_id=0000000000245 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added file-compress-rule compressor1 from GUI(172.20.120.47) "</pre>

Related

- [00050402](#)
- [00050411](#)

Table 467:

Meaning
An administrator changed a compressor.

Table 468:

Field name	Description
ID (log_id)	00050402 See “Log ID numbers” on page 23.

Table 469:

Example
<pre>date=2013-10-08 time=10:56:46 log_id=00050402 msg_id=0000000000246 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed file-compress-rule compressor1 from GUI(172.20.120.47) "</pre>

Related

- [00050401](#)
- [00050411](#)

00050411

Table 470:

Meaning
An administrator deleted a compressor.

Table 471:

Field name	Description
ID (log_id)	00050411 See “Log ID numbers” on page 23.

Table 472:

Example
<pre>date=2013-10-08 time=10:56:56 log_id=00050411 msg_id=000000000247 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted file-compress-rule compressor1 from GUI(172.20.120.47) "</pre>

Related

- [00050401](#)
- [00050402](#)

Table 473:

Meaning
An administrator created an HTTP flood prevention rule.

Table 474:

Field name	Description
ID (log_id)	00051001 See “Log ID numbers” on page 23.

Table 475:

Example
<pre>date=2013-10-08 time=10:40:19 log_id=00051001 msg_id=000000000175 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added http-request-flood-prevention-rule http-flood-ip1 from GUI(172.20.120.47) "</pre>

Related

- [00051002](#)
- [00051011](#)

Table 476:

Meaning
An administrator changed an HTTP flood prevention rule.

Table 477:

Field name	Description
ID (log_id)	00051002 See “Log ID numbers” on page 23.

Table 478:

Example
<pre>date=2013-10-10 time=00:36:04 log_id=00051002 msg_id=0000000000418 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed http-request-flood-prevention-rule http-flood-ip1 from GUI(172.20.120.47) "</pre>

Related

- [00051001](#)
- [00051011](#)

00051011

Table 479:

Meaning
An administrator deleted an HTTP flood prevention rule.

Table 480:

Field name	Description
ID (log_id)	00051011 See “Log ID numbers” on page 23.

Table 481:

Example
<pre>date=2013-10-10 time=00:36:24 log_id=00051011 msg_id=0000000000419 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted http-request-flood-prevention-rule http-flood-ip1 from GUI(172.20.120.47) "</pre>

Related

- [00051001](#)
- [00051002](#)

Table 482:

Meaning
An administrator created a malicious IPs rule.

Table 483:

Field name	Description
ID (log_id)	00051201 See “Log ID numbers” on page 23.

Table 484:

Example
<pre>date=2013-10-08 time=10:40:35 log_id=00051201 msg_id=000000000176 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added http-connection-flood-check-rule dos-ip1 from GUI(172.20.120.47) "</pre>

Related

- [00051202](#)
- [00051211](#)

Table 485:

Meaning
An administrator changed a malicious IPs rule.

Table 486:

Field name	Description
ID (log_id)	00051202 See “Log ID numbers” on page 23.

Table 487:

Example
<pre>date=2013-10-10 time=00:36:13 log_id=00051202 msg_id=0000000000419 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed http-connection-flood-check-rule dos-ip1 from GUI(172.20.120.47) "</pre>

Related

- [00051201](#)
- [00051211](#)

00051211

Table 488:

Meaning
An administrator deleted a malicious IPs rule.

Table 489:

Field name	Description
ID (log_id)	00051211 See “Log ID numbers” on page 23.

Table 490:

Example
<pre>date=2013-10-10 time=00:36:23 log_id=00051211 msg_id=0000000000420 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted http-connection-flood-check-rule dos-ip1 from GUI(172.20.120.47) "</pre>

Related

- [00051201](#)
- [00051202](#)

Table 491:

Meaning
An administrator created a HTTP access limit rule.

Table 492:

Field name	Description
ID (log_id)	00051401 See “Log ID numbers” on page 23.

Table 493:

Example
<pre>date=2013-10-08 time=10:40:35 log_id=00051401 msg_id=000000000176 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added layer4-access-limit-rule dos-ip1 from GUI(172.20.120.47) "</pre>

Related

- [00051402](#)
- [00051411](#)

Table 494:

Meaning
An administrator changed a HTTP access limit rule.

Table 495:

Field name	Description
ID (log_id)	00051402 See “Log ID numbers” on page 23.

Table 496:

Example
<pre>date=2013-10-10 time=00:36:13 log_id=00051402 msg_id=0000000000419 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed layer4-access-limit-rule dos-ip1 from GUI(172.20.120.47) "</pre>

Related

- [00051401](#)
- [00051411](#)

00051411

Table 497:

Meaning
An administrator deleted a HTTP access limit rule.

Table 498:

Field name	Description
ID (log_id)	00051411 See “Log ID numbers” on page 23.

Table 499:

Example
<pre>date=2013-10-10 time=00:36:23 log_id=00051411 msg_id=0000000000420 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted layer4-access-limit-rule dos-ip1 from GUI(172.20.120.47) "</pre>

Related

- [00051401](#)
- [00051402](#)

Table 500:

Meaning
An administrator created a TCP flood prevention rule.

Table 501:

Field name	Description
ID (log_id)	00051601 See “Log ID numbers” on page 23.

Table 502:

Example
<pre>date=2013-10-08 time=10:41:36 log_id=00051601 msg_id=000000000178 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added waf-layer4-connection-flood-check-rule tcp-flood-preventer1 from GUI(172.20.120.47) "</pre>

Related

- [00051602](#)
- [00051611](#)

Table 503:

Meaning
An administrator changed a TCP flood prevention rule.

Table 504:

Field name	Description
ID (log_id)	00051602 See “Log ID numbers” on page 23.

Table 505:

Example
<pre>date=2013-10-10 time=00:35:51 log_id=00051602 msg_id=0000000000417 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed waf-layer4-connection-flood-check-rule tcp-flood-preventer1 from GUI(172.20.120.47) "</pre>

Related

- [00051601](#)
- [00051611](#)

Table 506:

Meaning
An administrator deleted a TCP flood prevention rule.

Table 507:

Field name	Description
ID (log_id)	00051611 See “Log ID numbers” on page 23.

Table 508:

Example
<pre>date=2013-10-10 time=00:35:59 log_id=00051611 msg_id=0000000000418 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin changed waf-layer4-connection-flood-check-rule tcp-flood-preventer1 from GUI(172.20.120.47) "</pre>

Related

- [00051601](#)
- [00051602](#)

Table 509:

Meaning
An administrator created a DoS protection policy.

Table 510:

Field name	Description
ID (log_id)	00051801 See “Log ID numbers” on page 23.

Table 511:

Example
<pre>date=2013-10-08 time=10:38:42 log_id=00051801 msg_id=000000000173 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added DoS protection policy dos-protection1 from GUI(172.20.120.47) "</pre>

Related

- [00051802](#)
- [00051811](#)

Table 512:

Meaning
An administrator changed a DoS protection policy.

Table 513:

Field name	Description
ID (log_id)	00051802 See “Log ID numbers” on page 23.

Table 514:

Example
<pre>date=2013-10-08 time=10:41:46 log_id=00051802 msg_id=0000000000179 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed DoS protection policy dos-protection1 from GUI(172.20.120.47) "</pre>

Related

- [00051801](#)
- [00051811](#)

00051811

Table 515:

Meaning
An administrator deleted a DoS protection policy.

Table 516:

Field name	Description
ID (log_id)	00051811 See “Log ID numbers” on page 23.

Table 517:

Example
<pre>date=2013-10-08 time=10:41:56 log_id=00051811 msg_id=0000000000180 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted DoS protection policy dos-protection1 from GUI(172.20.120.47) "</pre>

Related

- [00051801](#)
- [00051802](#)

00052201

Table 518:

Meaning
An administrator created a client IP white list or black list.

Table 519:

Field name	Description
ID (log_id)	00052201 See “Log ID numbers” on page 23.

Table 520:

Example
<pre>date=2013-10-11 time=09:57:02 log_id=00052201 msg_id=0000000000460 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added waf ip-list blacklist from GUI(172.20.120.47) "</pre>

Related

- [00052202](#)
- [00052211](#)

Table 521:

Meaning
An administrator changed a client IP white list or black list.

Table 522:

Field name	Description
ID (log_id)	00052202 See “Log ID numbers” on page 23.

Table 523:

Example
<pre>date=2013-10-11 time=09:57:12 log_id=00052202 msg_id=0000000000461 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed waf ip-list blacklist from GUI(172.20.120.47) "</pre>

Related

- [00052201](#)
- [00052211](#)

Table 524:

Meaning
An administrator deleted a client IP white list or black list.

Table 525:

Field name	Description
ID (log_id)	00052211 See “Log ID numbers” on page 23.

Table 526:

Example
<pre>date=2013-10-11 time=09:57:22 log_id=00052211 msg_id=0000000000462 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted waf ip-list blacklist from GUI(172.20.120.47) "</pre>

Related

- [00052201](#)
- [00052202](#)

Table 527:

Meaning
An administrator created a user authentication rule.

Table 528:

Field name	Description
ID (log_id)	00052401 See “Log ID numbers” on page 23.

Table 529:

Example
<pre>date=2013-10-08 time=10:57:07 log_id=00052401 msg_id=0000000000254 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added http-authen-rule user-auth-realms 1 from GUI(172.20.120.47) "</pre>

Related

- [00052402](#)
- [00052411](#)

Table 530:

Meaning
An administrator changed a user authentication rule.

Table 531:

Field name	Description
ID (log_id)	00052402 See “Log ID numbers” on page 23.

Table 532:

Example
<pre>date=2013-10-08 time=10:57:33 log_id=00052402 msg_id=0000000000255 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed http-authen-rule user-auth-realms1 from GUI(172.20.120.47) "</pre>

Related

- [00052401](#)
- [00052411](#)

00052411

Table 533:

Meaning
An administrator deleted a user authentication rule.

Table 534:

Field name	Description
ID (log_id)	00052411 See “Log ID numbers” on page 23.

Table 535:

Example
<pre>date=2013-10-09 time=16:15:22 log_id=00052411 msg_id=0000000000316 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted http-authen-rule user-auth-realms1 from GUI(172.20.120.47) "</pre>

Related

- [00052401](#)
- [00052402](#)

Table 536:

Meaning
An administrator created a user authentication policy.

Table 537:

Field name	Description
ID (log_id)	00052601 See “Log ID numbers” on page 23.

Table 538:

Example
<pre>date=2013-10-08 time=10:57:59 log_id=00052601 msg_id=0000000000257 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added http-authen-policy user-auth-policy1 from GUI(172.20.120.47) "</pre>

Related

- [00052602](#)
- [00052611](#)

Table 539:

Meaning
An administrator changed a user authentication policy.

Table 540:

Field name	Description
ID (log_id)	00052602 See “Log ID numbers” on page 23.

Table 541:

Example
<pre>date=2013-10-08 time=10:58:02 log_id=00052602 msg_id=0000000000258 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed http-authen-policy user-auth-policy1 from GUI(172.20.120.47) "</pre>

Related

- [00052601](#)
- [00052611](#)

Table 542:

Meaning
An administrator deleted a user authentication policy.

Table 543:

Field name	Description
ID (log_id)	00052611 See “Log ID numbers” on page 23.

Table 544:

Example
<pre>date=2013-10-09 time=16:15:17 log_id=00052611 msg_id=0000000000315 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted http-authen-policy user-auth-connections-temp from GUI(172.20.120.47) "</pre>

Related

- [00052601](#)
- [00052602](#)

Table 545:

Meaning
An administrator added an input rule for HTTP requests.

Table 546:

Field name	Description
ID (log_id)	00053201 See “Log ID numbers” on page 23.

Table 547:

Example
<pre>date=2014-04-10 time=16:50:46 log_id=00053201 msg_id=000000734635 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added input-rule ddddd from GUI(172.22.6.237)"</pre>

Related

- [00053202](#)
- [00053211](#)

Table 548:

Meaning
An administrator edited an input rule for HTTP requests.

Table 549:

Field name	Description
ID (log_id)	00053202 See “Log ID numbers” on page 23.

Table 550:

Example
<pre>date=2014-04-10 time=16:54:39 log_id=00053202 msg_id=000000734636 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed input-rule ddddd from GUI(172.22.6.237)"</pre>

Related

- [00053201](#)
- [00053211](#)

Table 551:

Meaning
An administrator deleted an input rule for HTTP requests.

Table 552:

Field name	Description
ID (log_id)	00053211 See “Log ID numbers” on page 23.

Table 553:

Example
<pre>date=2014-04-10 time=16:56:42 log_id=00053211 msg_id=000000734637 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted input-rule ddddd from GUI(172.22.6.237)"</pre>

Related

- [00053201](#)
- [00053202](#)

Table 554:

Meaning
An administrator added a parameter validation rule.

Table 555:

Field name	Description
ID (log_id)	00053701 See “Log ID numbers” on page 23.

Table 556:

Example
<pre>date=2014-04-10 time=16:41:56 log_id=00053701 msg_id=000000734632 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added parameter-validation-rule 123 from GUI(172.22.6.237) "</pre>

Related

- [00053711](#)

00053711

Table 557:

Meaning
An administrator deleted a parameter validation rule.

Table 558:

Field name	Description
ID (log_id)	00053711 See “Log ID numbers” on page 23.

Table 559:

Example
<pre>date=2014-04-10 time=16:49:47 log_id=00053711 msg_id=000000734634 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted parameter-validation-rule 123 from GUI(172.22.6.237) "</pre>

Related

- [00053701](#)

Table 560:

Meaning
An administrator created a hidden input rule.

Table 561:

Field name	Description
ID (log_id)	00053901 See “Log ID numbers” on page 23.

Table 562:

Example
<pre>date=2013-10-08 time=10:51:19 log_id=00053901 msg_id=0000000000218 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added hidden-fields-rule hidden-input-rule1 from GUI(172.20.120.47) "</pre>

Related

- [00053902](#)
- [00053911](#)

Table 563:

Meaning
An administrator changed a hidden input rule.

Table 564:

Field name	Description
ID (log_id)	00053902 See “Log ID numbers” on page 23.

Table 565:

Example
<pre>date=2013-10-08 time=10:51:25 log_id=00053902 msg_id=0000000000219 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed hidden-fields-rule hidden-input-rule1 from GUI(172.20.120.47) "</pre>

Related

- [00053901](#)
- [00053911](#)

Table 566:

Meaning
An administrator deleted a hidden input rule.

Table 567:

Field name	Description
ID (log_id)	00053911 See “Log ID numbers” on page 23.

Table 568:

Example
<pre>date=2013-10-08 time=10:51:35 log_id=00053911 msg_id=000000000220 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted hidden-fields-rule hidden-input-rule1 from GUI(172.20.120.47) "</pre>

Related

- [00053901](#)
- [00053902](#)

00054401

Table 569:

Meaning
An administrator created a hidden input policy.

Table 570:

Field name	Description
ID (log_id)	00054401 See “Log ID numbers” on page 23.

Table 571:

Example
<pre>date=2013-10-08 time=10:52:11 log_id=00054401 msg_id=000000000222 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added hidden-fields-protection hidden-input-policy1 from GUI(172.20.120.47) "</pre>

Related

- [00054402](#)
- [00054411](#)

Table 572:

Meaning
An administrator changed a hidden input policy.

Table 573:

Field name	Description
ID (log_id)	00054402 See “Log ID numbers” on page 23.

Table 574:

Example
<pre>date=2013-10-08 time=10:52:16 log_id=00054402 msg_id=0000000000223 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed hidden-fields-protection hidden-input-policy1 from GUI(172.20.120.47) "</pre>

Related

- [00054401](#)
- [00054411](#)

00054411

Table 575:

Meaning
An administrator deleted a hidden input policy.

Table 576:

Field name	Description
ID (log_id)	00054411 See “Log ID numbers” on page 23.

Table 577:

Example
<pre>date=2013-10-08 time=10:52:26 log_id=00054411 msg_id=000000000224 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted hidden-fields-protection hidden-input-policy1 from GUI(172.20.120.47) "</pre>

Related

- [00054401](#)
- [00054402](#)

Table 578:

Meaning
An administrator created a page order rule.

Table 579:

Field name	Description
ID (log_id)	00054601 See “Log ID numbers” on page 23.

Table 580:

Example
<pre>date=2013-10-08 time=10:44:40 log_id=00054601 msg_id=0000000000191 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added page-access-rule page-order1 from GUI(172.20.120.47) "</pre>

Related

- [00054602](#)
- [00054611](#)

Table 581:

Meaning
An administrator changed a page order rule.

Table 582:

Field name	Description
ID (log_id)	00054602 See “Log ID numbers” on page 23.

Table 583:

Example
<pre>date=2013-10-08 time=10:44:49 log_id=00054602 msg_id=0000000000192 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed page-access-rule page-order1 from GUI(172.20.120.47) "</pre>

Related

- [00054601](#)
- [00054611](#)

00054611

Table 584:

Meaning
An administrator deleted a page order rule.

Table 585:

Field name	Description
ID (log_id)	00054611 See “Log ID numbers” on page 23.

Table 586:

Example
<pre>date=2013-10-08 time=10:44:49 log_id=00054611 msg_id=000000000193 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted page-access-rule page-order1 from GUI(172.20.120.47) "</pre>

Related

- [00054601](#)
- [00054602](#)

Table 587:

Meaning
An administrator created a rewrite/redirect rule.

Table 588:

Field name	Description
ID (log_id)	00054801 See “Log ID numbers” on page 23.

Table 589:

Example
<pre>date=2013-10-08 time=11:07:40 log_id=00054801 msg_id=0000000000263 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added url-rewrite-rule http-to-https-redirect from GUI(172.20.120.47) "</pre>

Related

- [00054802](#)
- [00054811](#)

Table 590:

Meaning
An administrator changed a rewrite/redirect rule.

Table 591:

Field name	Description
ID (log_id)	00054802 See “Log ID numbers” on page 23.

Table 592:

Example
<pre>date=2013-10-08 time=11:07:55 log_id=00054802 msg_id=0000000000264 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed url-rewrite-rule http-to-https-redirect from GUI(172.20.120.47) "</pre>

Related

- [00054801](#)
- [00054811](#)

Table 593:

Meaning
An administrator deleted a rewrite/redirect rule.

Table 594:

Field name	Description
ID (log_id)	00054811 See “Log ID numbers” on page 23.

Table 595:

Example
<pre>date=2013-10-08 time=11:08:55 log_id=00054811 msg_id=0000000000265 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted url-rewrite-rule http-to-https-redirect from GUI(172.20.120.47) "</pre>

Related

- [00054801](#)
- [00054802](#)

Table 596:

Meaning
An administrator created a rewrite/redirect policy.

Table 597:

Field name	Description
ID (log_id)	00055301 See “Log ID numbers” on page 23.

Table 598:

Example
<pre>date=2013-10-08 time=11:09:10 log_id=00055301 msg_id=0000000000268 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added url-rewrite-policy request-rewrites1 from GUI(172.20.120.47) "</pre>

Related

- [00055302](#)
- [00055311](#)

Table 599:

Meaning
An administrator changed a rewrite/redirect policy.

Table 600:

Field name	Description
ID (log_id)	00055302 See “Log ID numbers” on page 23.

Table 601:

Example
<pre>date=2013-10-08 time=11:09:14 log_id=00055302 msg_id=0000000000269 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed url-rewrite-policy request-rewrites1 from GUI(172.20.120.47) "</pre>

Related

- [00055301](#)
- [00055311](#)

Table 602:

Meaning
An administrator deleted a rewrite/redirect policy.

Table 603:

Field name	Description
ID (log_id)	00055311 See “Log ID numbers” on page 23.

Table 604:

Example
<pre>date=2013-10-08 time=11:09:34 log_id=00055311 msg_id=0000000000270 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted url-rewrite-policy request-rewrites1 from GUI(172.20.120.47) "</pre>

Related

- [00055301](#)
- [00055302](#)

00055501

Table 605:

Meaning
An administrator created an allowed HTTP method exception.

Table 606:

Field name	Description
ID (log_id)	00055501 See “Log ID numbers” on page 23.

Table 607:

Example
<pre>date=2013-10-08 time=10:42:10 log_id=00055501 msg_id=0000000000180 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added allow-method-exceptions method-exempt1 from GUI(172.20.120.47) "</pre>

Related

- [00055502](#)
- [00055511](#)

Table 608:

Meaning
An administrator changed an allowed HTTP method exception.

Table 609:

Field name	Description
ID (log_id)	00055502 See “Log ID numbers” on page 23.

Table 610:

Example
<pre>date=2013-10-08 time=10:42:33 log_id=00055502 msg_id=0000000000181 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed allow-method-exceptions method-exempt1 from GUI(172.20.120.47) "</pre>

Related

- [00055501](#)
- [00055511](#)

00055511

Table 611:

Meaning
An administrator deleted an allowed HTTP method exception.

Table 612:

Field name	Description
ID (log_id)	00055511 See “Log ID numbers” on page 23.

Table 613:

Example
<pre>date=2013-10-08 time=10:42:43 log_id=00055511 msg_id=000000000182 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted allow-method-exceptions method-exempt1 from GUI(172.20.120.47) "</pre>

Related

- [00055501](#)
- [00055502](#)

Table 614:

Meaning
An administrator created an allowed HTTP method.

Table 615:

Field name	Description
ID (log_id)	00055701 See “Log ID numbers” on page 23.

Table 616:

Example
<pre>date=2013-10-08 time=10:43:04 log_id=00055701 msg_id=0000000000183 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added allow-method-policy allowed-methods1 from GUI(172.20.120.47) "</pre>

Related

- [00055702](#)
- [00055711](#)

Table 617:

Meaning
An administrator changed an allowed HTTP method.

Table 618:

Field name	Description
ID (log_id)	00055702 See “Log ID numbers” on page 23.

Table 619:

Example
<pre>date=2013-10-08 time=10:43:14 log_id=00055702 msg_id=0000000000184 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed allow-method-policy allowed-methods1 from GUI(172.20.120.47) "</pre>

Related

- [00055701](#)
- [00055711](#)

00055711

Table 620:

Meaning
An administrator deleted an allowed HTTP method.

Table 621:

Field name	Description
ID (log_id)	00055711 See “Log ID numbers” on page 23.

Table 622:

Example
<pre>date=2013-10-08 time=10:43:24 log_id=00055711 msg_id=0000000000185 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted allow-method-policy allowed-methods1 from GUI(172.20.120.47) "</pre>

Related

- [00055701](#)
- [00055702](#)

00055901

Table 623:

Meaning
An administrator created an access control rule.

Table 624:

Field name	Description
ID (log_id)	00055901 See “Log ID numbers” on page 23.

Table 625:

Example
<pre>date=2013-10-08 time=10:46:02 log_id=00055901 msg_id=0000000000196 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added url-access-rule access-control1 from GUI(172.20.120.47) "</pre>

Related

- [00055902](#)
- [00055911](#)

Table 626:

Meaning
An administrator changed an access control rule.

Table 627:

Field name	Description
ID (log_id)	00055902 See “Log ID numbers” on page 23.

Table 628:

Example
<pre>date=2013-10-08 time=10:46:12 log_id=00055902 msg_id=0000000000197 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed url-access-rule access-control1 from GUI(172.20.120.47) "</pre>

Related

- [00055901](#)
- [00055911](#)

Table 629:

Meaning
An administrator deleted an access control rule.

Table 630:

Field name	Description
ID (log_id)	00055911 See “Log ID numbers” on page 23.

Table 631:

Example
<pre>date=2013-10-08 time=10:46:22 log_id=00055911 msg_id=0000000000198 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted url-access-rule access-control1 from GUI(172.20.120.47) "</pre>

Related

- [00055901](#)
- [00055902](#)

00056401

Table 632:

Meaning
An administrator created an access control policy.

Table 633:

Field name	Description
ID (log_id)	00056401 See “Log ID numbers” on page 23.

Table 634:

Example
<pre>date=2013-10-08 time=10:46:42 log_id=00056401 msg_id=000000000199 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added url-access-policy access-control-group1 from GUI(172.20.120.47) "</pre>

Related

- [00056402](#)
- [00056411](#)

Table 635:

Meaning
An administrator changed an access control policy.

Table 636:

Field name	Description
ID (log_id)	00056402 See “Log ID numbers” on page 23.

Table 637:

Example
<pre>date=2013-10-08 time=10:47:04 log_id=00056402 msg_id=0000000000202 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed url-access-policy access-control-group1 from GUI(172.20.120.47) "</pre>

Related

- [00056401](#)
- [00056411](#)

Table 638:

Meaning
An administrator deleted an access control policy.

Table 639:

Field name	Description
ID (log_id)	00056411 See “Log ID numbers” on page 23.

Table 640:

Example
<pre>date=2013-10-08 time=10:47:14 log_id=00056411 msg_id=0000000000203 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted url-access-policy access-control-group1 from GUI(172.20.120.47) "</pre>

Related

- [00056401](#)
- [00056402](#)

00056601

Table 641:

Meaning
An administrator created an HTTP constraint.

Table 642:

Field name	Description
ID (log_id)	00056601 See “Log ID numbers” on page 23.

Table 643:

Example
<pre>date=2013-10-08 time=10:48:21 log_id=00056601 msg_id=0000000000207 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added http-protocol-parameter-restriction http-contraints1 from GUI(172.20.120.47) "</pre>

Related

- [00056602](#)
- [00056611](#)

Table 644:

Meaning
An administrator changed an HTTP constraint.

Table 645:

Field name	Description
ID (log_id)	00056602 See “Log ID numbers” on page 23.

Table 646:

Example
<pre>date=2013-10-11 time=10:17:50 log_id=00056602 msg_id=0000000000482 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed http-protocol-parameter-restriction http-contraints1 from GUI(172.20.120.47) "</pre>

Related

- [00056601](#)
- [00056611](#)

00056611

Table 647:

Meaning
An administrator deleted an HTTP constraint.

Table 648:

Field name	Description
ID (log_id)	00056611 See “Log ID numbers” on page 23.

Table 649:

Example
<pre>date=2013-10-11 time=10:17:59log_id=00056611 msg_id=0000000000483 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted http-protocol-parameter-restriction http-contraints1 from GUI(172.20.120.47) "</pre>

Related

- [00056601](#)
- [00056602](#)

00058601

Table 650:

Meaning
An administrator created an HTTP constraint exemption.

Table 651:

Field name	Description
ID (log_id)	00058601 See “Log ID numbers” on page 23.

Table 652:

Example
<pre>date=2013-10-08 time=10:47:28 log_id=00058601 msg_id=0000000000204 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added http-constraints-exception http-constraints-exempt1 from GUI(172.20.120.47) "</pre>

Related

- [00058602](#)
- [00058611](#)

Table 653:

Meaning
An administrator changed an HTTP constraint exemption.

Table 654:

Field name	Description
ID (log_id)	00058602 See “Log ID numbers” on page 23.

Table 655:

Example
<pre>date=2013-10-08 time=10:47:51 log_id=00058602 msg_id=0000000000205 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed http-constraints-exception http-constraints-exempt1 from GUI(172.20.120.47) "</pre>

Related

- [00058601](#)
- [00058611](#)

00058611

Table 656:

Meaning
An administrator deleted an HTTP constraint exemption.

Table 657:

Field name	Description
ID (log_id)	00058611 See “Log ID numbers” on page 23.

Table 658:

Example
<pre>date=2013-10-08 time=10:48:51 log_id=00058611 msg_id=0000000000206 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted http-constraints-exception http-constraints-exempt1 from GUI(172.20.120.47) "</pre>

Related

- [00058601](#)
- [00058602](#)

Table 659:

Meaning
An administrator created a custom signature.

Table 660:

Field name	Description
ID (log_id)	00059801 See “Log ID numbers” on page 23.

Table 661:

Example
<pre>date=2013-10-08 time=10:54:06 log_id=00059801 msg_id=0000000000232 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-protection-rule custom-signature1 from GUI(172.20.120.47) "</pre>

Related

- [00059802](#)
- [00059811](#)

Table 662:

Meaning
An administrator changed a custom signature.

Table 663:

Field name	Description
ID (log_id)	00059802 See “Log ID numbers” on page 23.

Table 664:

Example
<pre>date=2013-10-08 time=10:54:22 log_id=00059802 msg_id=0000000000233 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-protection-rule custom-signature1 from GUI(172.20.120.47) "</pre>

Related

- [00059801](#)
- [00059811](#)

Table 665:

Meaning
An administrator deleted a custom signature.

Table 666:

Field name	Description
ID (log_id)	00059811 See “Log ID numbers” on page 23.

Table 667:

Example
<pre>date=2013-10-08 time=10:55:25 log_id=00059811 msg_id=0000000000239 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted custom-protection-rule custom-signature2 from GUI(172.20.120.47) "</pre>

Related

- [00059801](#)
- [00059802](#)

00060001

Table 668:

Meaning
An administrator created a group of custom signatures.

Table 669:

Field name	Description
ID (log_id)	00060001 See “Log ID numbers” on page 23.

Table 670:

Example
<pre>date=2013-10-08 time=10:54:46 log_id=00060001 msg_id=000000000235 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-protection-group custom-signatures1 from GUI(172.20.120.47) "</pre>

Related

- [00060002](#)
- [00060011](#)

Table 671:

Meaning
An administrator changed a group of custom signatures.

Table 672:

Field name	Description
ID (log_id)	00060002 See “Log ID numbers” on page 23.

Table 673:

Example
<pre>date=2013-10-08 time=10:54:51 log_id=00060002 msg_id=0000000000236 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-protection-group custom-signatures1 from GUI(172.20.120.47) "</pre>

Related

- [00060001](#)
- [00060011](#)

00060011

Table 674:

Meaning
An administrator deleted a group of custom signatures.

Table 675:

Field name	Description
ID (log_id)	00060011 See “Log ID numbers” on page 23.

Table 676:

Example
<pre>date=2013-10-08 time=10:55:51 log_id=00060011 msg_id=0000000000237 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=delstatus=success msg="User admin deleted custom-protection-group custom-signatures1 from GUI(172.20.120.47) "</pre>

Related

- [00060001](#)
- [00060002](#)

00060201

Table 677:

Meaning
An administrator created an attack signatures rule.

Table 678:

Field name	Description
ID (log_id)	00060201 See “Log ID numbers” on page 23.

Table 679:

Example
<pre>date=2013-10-17 time=21:58:28 log_id=00060201 msg_id=0000000000762 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added signature attack-signatures2 from GUI(192.168.1.28) "</pre>

Related

- [00060202](#)
- [00060211](#)

Table 680:

Meaning
An administrator changed an attack signatures rule.

Table 681:

Field name	Description
ID (log_id)	00060202 See “Log ID numbers” on page 23.

Table 682:

Example
<pre>date=2013-10-17 time=21:47:39 log_id=00060202 msg_id=0000000000759 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed signature attack-signatures1 from GUI(192.168.1.28) "</pre>

Related

- [00060201](#)
- [00060211](#)

00060211

Table 683:

Meaning
An administrator deleted an attack signatures rule.

Table 684:

Field name	Description
ID (log_id)	00060211 See “Log ID numbers” on page 23.

Table 685:

Example
<pre>date=2013-10-17 time=21:58:46 log_id=00060211 msg_id=0000000000763 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted signature attack-signatures2 from GUI(192.168.1.28) "</pre>

Related

- [00060201](#)
- [00060202](#)

Table 686:

Meaning
An administrator created an X-Forwarded-For : rule.

Table 687:

Field name	Description
ID (log_id)	00061201 See “Log ID numbers” on page 23.

Table 688:

Example
<pre>date=2013-10-17 time=22:04:30 log_id=00061201 msg_id=0000000000764 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added x-forwarded-for xff1 from GUI(192.168.1.28) "</pre>

Related

- [00061202](#)
- [00061211](#)

Table 689:

Meaning
An administrator changed an X-Forwarded-For : rule.

Table 690:

Field name	Description
ID (log_id)	00061202 See “Log ID numbers” on page 23.

Table 691:

Example
<pre>date=2013-10-17 time=22:04:35 log_id=00061202 msg_id=0000000000765 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed x-forwarded-for xff1 from GUI(192.168.1.28) "</pre>

Related

- [00061201](#)
- [00061211](#)

00061211

Table 692:

Meaning
An administrator deleted an X-Forwarded-For : rule.

Table 693:

Field name	Description
ID (log_id)	00061211 See “Log ID numbers” on page 23.

Table 694:

Example
<pre>date=2013-10-17 time=22:04:44 log_id=00061211 msg_id=0000000000766 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted x-forwarded-for xff1 from GUI(192.168.1.28) "</pre>

Related

- [00061201](#)
- [00061202](#)

00061401

Table 695:

Meaning
An administrator created a session initiation rule ("start page rule").

Table 696:

Field name	Description
ID (log_id)	00061401 See "Log ID numbers" on page 23.

Table 697:

Example
<pre>date=2013-10-08 time=10:43:33 log_id=00061401 msg_id=0000000000184 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added start-pages session-init-page1 from GUI(172.20.120.47) "</pre>

Related

- [00061402](#)
- [00061411](#)

Table 698:

Meaning
An administrator changed a session initiation rule ("start page rule").

Table 699:

Field name	Description
ID (log_id)	00061402 See "Log ID numbers" on page 23.

Table 700:

Example
<pre>date=2013-10-08 time=10:43:46 log_id=00061402 msg_id=0000000000185 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed start-pages session-init-page1 from GUI(172.20.120.47) "</pre>

Related

- [00061401](#)
- [00061411](#)

00061411

Table 701:

Meaning
An administrator deleted a session initiation rule ("start page rule").

Table 702:

Field name	Description
ID (log_id)	00061411 See "Log ID numbers" on page 23.

Table 703:

Example
<pre>date=2013-10-08 time=10:43:56 log_id=00061411 msg_id=000000000186 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted start-pages session-init-page1 from GUI(172.20.120.47) "</pre>

Related

- [00061401](#)
- [00061402](#)

Table 704:

Meaning
An administrator has added a brute force login attack profile.

Table 705:

Field name	Description
ID (log_id)	00061801 See “Log ID numbers” on page 23.

Table 706:

Example
<pre>date=2014-04-10 time=10:38:38 log_id=00061801 msg_id=000000055127 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added waf-brute-force-login dwg from GUI(172.22.6.149) "</pre>

Related

- [00061802](#)
- [00061811](#)

Table 707:

Meaning
An administrator edited a brute force login attack profile.

Table 708:

Field name	Description
ID (log_id)	00061802 See “Log ID numbers” on page 23.

Table 709:

Example
<pre>date=2014-04-10 time=11:15:21 log_id=00061802 msg_id=000000055128 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed waf-brute-force-login dwg from GUI(172.22.6.149) "</pre>

Related

- [00061801](#)
- [00061811](#)

00061811

Related

Table 710:

Meaning
An administrator has edited a brute force login attack profile.

Table 711:

Field name	Description
ID (log_id)	00061811 See “Log ID numbers” on page 23.

Table 712:

Example
<pre>date=2014-04-10 time=11:15:47 log_id=00061811 msg_id=000000055129 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted waf-brute-force-login dwg from GUI(172.22.6.149) "</pre>

- [00061801](#)
- [00061802](#)

Table 713:

Meaning
An administrator created an upload restriction rule.

Table 714:

Field name	Description
ID (log_id)	00062001 See “Log ID numbers” on page 23.

Table 715:

Example
<pre>date=2013-10-08 time=10:49:10 log_id=00062001 msg_id=0000000000208 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added file-upload-restriction-rule video-uploads-limit1 from GUI(172.20.120.47) "</pre>

Related

- [00062002](#)
- [00062011](#)

Table 716:

Meaning
An administrator changed an upload restriction rule.

Table 717:

Field name	Description
ID (log_id)	00062002 See “Log ID numbers” on page 23.

Table 718:

Example
<pre>date=2013-10-08 time=10:49:49 log_id=00062002 msg_id=0000000000209 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed file-upload-restriction-rule video-uploads-limit1 from GUI(172.20.120.47) "</pre>

Related

- [00062001](#)
- [00062011](#)

Table 719:

Meaning
An administrator deleted an upload restriction rule.

Table 720:

Field name	Description
ID (log_id)	00062011 See “Log ID numbers” on page 23.

Table 721:

Example
<pre>date=2013-10-08 time=10:49:59 log_id=00062011 msg_id=0000000000210 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted file-upload-restriction-rule video-uploads-limit1 from GUI(172.20.120.47) "</pre>

Related

- [00062001](#)
- [00062002](#)

Table 722:

Meaning
An administrator created an upload restriction policy.

Table 723:

Field name	Description
ID (log_id)	00062201 See “Log ID numbers” on page 23.

Table 724:

Example
<pre>date=2013-10-17 time=22:27:13 log_id=00062201 msg_id=0000000000770 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added waf-file-upload-restriction-policy all-file-uploads1 from GUI(192.168.1.28) "</pre>

Related

- [00062202](#)
- [00062011](#)

Table 725:

Meaning
An administrator changed an upload restriction policy.

Table 726:

Field name	Description
ID (log_id)	00062202 See “Log ID numbers” on page 23.

Table 727:

Example
<pre>date=2013-10-17 time=22:27:24 log_id=00062202 msg_id=000000000772 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed waf-file-upload-restriction-policy all-file-uploads1 from GUI(192.168.1.28) "</pre>

Related

- [00062201](#)
- [00062211](#)

00062211

Table 728:

Meaning
An administrator deleted an upload restriction policy.

Table 729:

Field name	Description
ID (log_id)	00062211 See “Log ID numbers” on page 23.

Table 730:

Example
<pre>date=2013-10-17 time=22:27:32 log_id=00062211 msg_id=0000000000773 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted waf-file-upload-restriction-policy file-uploads from GUI(192.168.1.28) "</pre>

Related

- [00062201](#)
- [00062202](#)

00062401

Table 731:

Meaning
An administrator created an inline protection profile.

Table 732:

Field name	Description
ID (log_id)	00062401 See “Log ID numbers” on page 23.

Table 733:

Example
<pre>date=2013-10-08 time=10:09:59 log_id=00062401 msg_id=00000000000088 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added inline-protection inline-protection-profile1 from GUI(172.20.120.47) "</pre>

Related

- [00062402](#)
- [00062411](#)

Table 734:

Meaning
An administrator changed an inline protection profile.

Table 735:

Field name	Description
ID (log_id)	00062402 See “Log ID numbers” on page 23.

Table 736:

Example
<pre>date=2013-10-10 time=00:32:06 log_id=00062402 msg_id=0000000000377 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed inline-protection inline-protection-profile1 from GUI(172.20.120.47) "</pre>

Related

- [00062401](#)
- [00062411](#)

00062411

Table 737:

Meaning
An administrator deleted an inline protection profile.

Table 738:

Field name	Description
ID (log_id)	00062411 See “Log ID numbers” on page 23.

Table 739:

Example
<pre>date=2013-10-08 time=10:18:34 log_id=00062411 msg_id=000000000118 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted inline-protection temp from GUI(172.20.120.47) "</pre>

Related

- [00062401](#)
- [00062402](#)

Table 740:

Meaning
An administrator created an offline protection profile.

Table 741:

Field name	Description
ID (log_id)	00063401 See “Log ID numbers” on page 23.

Table 742:

Example
<pre>date=2013-10-08 time=10:18:44 log_id=00063401 msg_id=0000000000119 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added offline-protection temp from GUI(172.20.120.47) "</pre>

Related

- [00063402](#)
- [00063411](#)

Table 743:

Meaning
An administrator changed an offline protection profile.

Table 744:

Field name	Description
ID (log_id)	00063402 See “Log ID numbers” on page 23.

Table 745:

Example
<pre>date=2013-10-08 time=10:18:49 log_id=00063402 msg_id=0000000000120 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed offline-protection temp from GUI(172.20.120.47) "</pre>

Related

- [00063401](#)
- [00063411](#)

Table 746:

Meaning
An administrator deleted an offline protection profile.

Table 747:

Field name	Description
ID (log_id)	00063411 See “Log ID numbers” on page 23.

Table 748:

Example
<pre>date=2013-10-08 time=10:18:53 log_id=00063411 msg_id=0000000000121 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted offline-protection temp from GUI(172.20.120.47) "</pre>

Related

- [00063401](#)
- [00063402](#)

00064401

Table 749:

Meaning
An administrator created an auto-learning profile.

Table 750:

Field name	Description
ID (log_id)	00064401 See “Log ID numbers” on page 23.

Table 751:

Example
<pre>date=2013-10-08 time=10:37:50 log_id=00064401 msg_id=0000000000166 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added autolearning-profile auto-learning1 from GUI(172.20.120.47) "</pre>

Related

- [00064402](#)
- [00064411](#)

Table 752:

Meaning
An administrator changed an auto-learning profile.

Table 753:

Field name	Description
ID (log_id)	00064402 See “Log ID numbers” on page 23.

Table 754:

Example
<pre>date=2013-10-15 time=20:31:30 log_id=00064402 msg_id=0000000000643 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed autolearning-profile auto-learning2 from GUI(192.168.1.28) "</pre>

Related

- [00064401](#)
- [00064411](#)

00064411

Table 755:

Meaning
An administrator deleted an auto-learning profile.

Table 756:

Field name	Description
ID (log_id)	00064411 See “Log ID numbers” on page 23.

Table 757:

Example
<pre>date=2013-10-15 time=20:31:37 log_id=00064411 msg_id=0000000000644 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted autolearning-profile auto-learning2 from GUI(192.168.1.28) "</pre>

Related

- [00064401](#)
- [00064402](#)

00065002

Table 758:

Meaning
An administrator changed an IP reputation setting.

Table 759:

Field name	Description
ID (log_id)	00065002 See “Log ID numbers” on page 23.

Table 760:

Example
<pre>date=2013-10-08 time=10:38:03 log_id=00065002 msg_id=0000000000171 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed IP Reputation from GUI(172.20.120.47) "</pre>

Table 761:

Meaning
An administrator created an IP reputation exemption.

Table 762:

Field name	Description
ID (log_id)	00065501 See “Log ID numbers” on page 23.

Table 763:

Example
<pre>date=2013-10-08 time=10:38:14 log_id=00065501 msg_id=000000000172 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added IP Reputation Exception 1 from GUI(172.20.120.47) "</pre>

Related

- [00065502](#)
- [00065511](#)

Table 764:

Meaning
An administrator changed an IP reputation exemption.

Table 765:

Field name	Description
ID (log_id)	00065502 See “Log ID numbers” on page 23.

Table 766:

Example
<pre>date=2013-10-17 time=22:51:51 log_id=00065502 msg_id=0000000000789 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed IP Reputation Exception 2 from GUI(192.168.1.28) "</pre>

Related

- [00065501](#)
- [00065511](#)

00065511

Table 767:

Meaning
An administrator deleted an IP reputation exemption.

Table 768:

Field name	Description
ID (log_id)	00065511 See “Log ID numbers” on page 23.

Table 769:

Example
<pre>date=2013-10-17 time=22:51:54 log_id=00065511 msg_id=0000000000790 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted IP Reputation Exception 2 from GUI(192.168.1.28) "</pre>

Related

- [00065501](#)
- [00065502](#)

00068001

Table 770:

Meaning
An administrator created a combination access control and rate limit rule ("custom rule").

Table 771:

Field name	Description
ID (log_id)	00068001 See "Log ID numbers" on page 23.

Table 772:

Example
<pre>date=2014-04-21 time=18:19:40 log_id=00068001 msg_id=0000000047914 device_id=FV400C3M12000060 vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-rule Custom_rule_for_PNG_server1 from GUI(172.22.6.231) "</pre>

Related

- [00068002](#)
- [00068011](#)

Table 773:

Meaning
An administrator changed a combination access control and rate limit rule ("custom rule").

Table 774:

Field name	Description
ID (log_id)	00068002 See "Log ID numbers" on page 23.

Table 775:

Example
<pre>date=2013-10-11 time=09:21:30 log_id=00068002 msg_id=0000000000441 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-rule combo-IP-rate1 from GUI(172.20.120.47) "</pre>

Related

- [00068002](#)
- [00068011](#)

00068011

Table 776:

Meaning
An administrator deleted a combination access control and rate limit rule ("custom rule").

Table 777:

Field name	Description
ID (log_id)	00068011 See "Log ID numbers" on page 23.

Table 778:

Example
<pre>date=2013-10-11 time=09:21:40 log_id=00068011 msg_id=0000000000442 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted custom-rule combo-IP-rate1 from GUI(172.20.120.47) "</pre>

Related

- [00068001](#)
- [00068002](#)

Table 779:

Meaning
An administrator created a combination access control and rate limit policy ("custom policy").

Table 780:

Field name	Description
ID (log_id)	00068301 See "Log ID numbers" on page 23.

Table 781:

Example
<pre>date=2014-04-21 time=18:25:26 log_id=00068301 msg_id=0000000047918 device_id=FV400C3M12000060 vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-policy Custom_Policy_For_PNG from GUI(172.22.6.231) "</pre>

Related

- [00068302](#)
- [00068311](#)

Table 782:

Meaning
An administrator changed a combination access control and rate limit policy ("custom policy").

Table 783:

Field name	Description
ID (log_id)	00068302 See "Log ID numbers" on page 23.

Table 784:

Example
<pre>date=2013-10-08 time=10:53:29 log_id=00068302 msg_id=0000000000230 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-policy combo-access-controls1 from GUI(172.20.120.47) "</pre>

Related

- [00068301](#)
- [00068311](#)

Table 785:

Meaning
An administrator deleted a combination access control and rate limit policy ("custom policy").

Table 786:

Field name	Description
ID (log_id)	00068311 See "Log ID numbers" on page 23.

Table 787:

Example
<pre>date=2013-10-08 time=10:53:39 log_id=00068311 msg_id=0000000000231 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted custom-policy combo-access-controls1 from GUI(172.20.120.47) "</pre>

Related

- [00068301](#)
- [00068302](#)

Table 788:

Meaning
An administrator has added an padding oracle rule.

Table 789:

Field name	Description
ID (log_id)	00068401 See “Log ID numbers” on page 23.

Table 790:

Example
<pre>date=2014-04-10 time=18:19:31 log_id=00068401 msg_id=000000820334 device_id=FVVM020000018475 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added waf-padding-oracle padding_001 from GUI(172.22.6.230) "</pre>

Related

- [00068402](#)
- [00068411](#)

Table 791:

Meaning
An administrator edited an padding oracle rule.

Table 792:

Field name	Description
ID (log_id)	00068402 See “Log ID numbers” on page 23.

Table 793:

Example
<pre>date=2014-04-10 time=18:24:59 log_id=00068402 msg_id=000000820335 device_id=FVVM020000018475 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed waf-padding-oracle padding_001 from GUI(172.22.6.230) "</pre>

Related

- [00068401](#)
- [00068411](#)

Table 794:

Meaning
An administrator deleted an padding oracle rule.

Table 795:

Field name	Description
ID (log_id)	00068411 See “Log ID numbers” on page 23.

Table 796:

Example
<pre>date=2014-04-10 time=18:26:05 log_id=00068411 msg_id=000000820336 device_id=FVVM020000018475 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted waf-padding-oracle padding_001 from GUI(172.22.6.230) "</pre>

Related

- [00068401](#)
- [00068402](#)

Table 797:

Meaning
An administrator added a web cache policy exception.

Table 798:

Field name	Description
ID (log_id)	00068701 See “Log ID numbers” on page 23.

Table 799:

Example
<pre>date=2014-04-10 time=16:44:43 log_id=00068701 msg_id=000000179517 device_id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added web-cache-exception ddd from GUI(172.22.6.66) "</pre>

Related

- [00068711](#)
- [00068801](#)
- [00068802](#)
- [00068811](#)

00068711

Table 800:

Meaning
An administrator deleted a web cache policy exception.

Table 801:

Field name	Description
ID (log_id)	00068711 See “Log ID numbers” on page 23.

Table 802:

Example
<pre>date=2014-09-11 time=02:00:30 log_id=00068711 msg_id=000003041973 device_id=FV400C3M14000006 vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted web-cache-exception ddd from GUI(172.22.14.6) "</pre>

Related

- [00068701](#)
- [00068801](#)
- [00068802](#)
- [00068811](#)

Table 803:

Meaning
An administrator added a web cache policy.

Table 804:

Field name	Description
ID (log_id)	00068801 See “Log ID numbers” on page 23.

Table 805:

Example
<pre>date=2014-04-10 time=16:41:57 log_id=00068801 msg_id=000000179514 device_id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added web-cache-policy FWB_web_cache from GUI(172.22.6.66) "</pre>

Related

- [00068802](#)
- [00068811](#)
- [00068701](#)
- [00068711](#)

Table 806:

Meaning
An administrator changed a web cache policy.

Table 807:

Field name	Description
ID (log_id)	00068802 See “Log ID numbers” on page 23.

Table 808:

Example
<pre>date=2014-04-10 time=16:43:10 log_id=00068802 msg_id=000000179515 device_id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed web-cache-policy FWB_web_cache from GUI(172.22.6.66) "</pre>

Related

- [00068801](#)
- [00068811](#)
- [00068701](#)
- [00068711](#)

Table 809:

Meaning
An administrator deleted a web cache policy.

Table 810:

Field name	Description
ID (log_id)	00068811 See “Log ID numbers” on page 23.

Table 811:

Example
<pre>date=2014-04-10 time=16:43:41 log_id=00068811 msg_id=000000179516 device_id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted web-cache-policy FWB_web_cache from GUI(172.22.6.66) "</pre>

Related

- [00068801](#)
- [00068802](#)
- [00068701](#)
- [00068711](#)

00090001

Table 812:

Meaning
An administrator created a vulnerability scan schedule.

Table 813:

Field name	Description
ID (log_id)	00090001 See “Log ID numbers” on page 23.

Table 814:

Example
<pre>date=2013-10-08 time=10:24:24 log_id=00090001 msg_id=0000000000140 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added wvs schedule vuln-scan-schedule1 from GUI(172.20.120.47) "</pre>

Related

- [00090002](#)
- [00090011](#)

00090002

Table 815:

Meaning
An administrator changed a vulnerability scan schedule.

Table 816:

Field name	Description
ID (log_id)	00090002 See “Log ID numbers” on page 23.

Table 817:

Example
<pre>date=2013-10-08 time=10:24:34 log_id=00090002 msg_id=0000000000141 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed wvs schedule vuln-scan-schedule1 from GUI(172.20.120.47) "</pre>

Related

- [00090001](#)
- [00090011](#)

00090011

Table 818:

Meaning
An administrator deleted a vulnerability scan schedule.

Table 819:

Field name	Description
ID (log_id)	00090011 See “Log ID numbers” on page 23.

Table 820:

Example
<pre>date=2013-10-08 time=10:24:44 log_id=00090011 msg_id=0000000000142 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted wvs schedule vuln-scan-schedule1 from GUI(172.20.120.47) "</pre>

Related

- [00090001](#)
- [00090002](#)

00090101

Table 821:

Meaning
An administrator created a vulnerability scan profile.

Table 822:

Field name	Description
ID (log_id)	00090101 See “Log ID numbers” on page 23.

Table 823:

Example
<pre>date=2014-04-10 time=17:38:53 log_id=00090101 msg_id=000000734654 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added wvs profile ddddd from GUI(172.22.6.237) "</pre>

Related

- [00090102](#)
- [00090111](#)

Table 824:

Meaning
An administrator changed a vulnerability scan profile.

Table 825:

Field name	Description
ID (log_id)	00090102 See “Log ID numbers” on page 23.

Table 826:

Example
<pre>date=2013-10-08 time=10:29:10 log_id=00090102 msg_id=0000000000144 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed wvs profile vuln-scan-profile1 from GUI(172.20.120.47) "</pre>

Related

- [00090101](#)
- [00090111](#)

00090111

Table 827:

Meaning
An administrator deleted a vulnerability scan profile.

Table 828:

Field name	Description
ID (log_id)	00090111 See “Log ID numbers” on page 23.

Table 829:

Example
<pre>date=2014-04-10 time=17:42:52 log_id=00090111 msg_id=000000734655 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted wvs profile ddddd from GUI(172.22.6.237) "</pre>

Related

- [00090101](#)
- [00090102](#)

00091101

Table 830:

Meaning
An administrator created a vulnerability scan policy.

Table 831:

Field name	Description
ID (log_id)	00091101 See “Log ID numbers” on page 23.

Table 832:

Example
<pre>date=2013-10-08 time=10:29:40 log_id=00091101 msg_id=000000000144 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added wvs policy vulnscan1 from GUI(172.20.120.47) "</pre>

Related

- [00091102](#)
- [00091111](#)

Table 833:

Meaning
An administrator changed a vulnerability scan policy.

Table 834:

Field name	Description
ID (log_id)	00091102 See “Log ID numbers” on page 23.

Table 835:

Example
<pre>date=2013-10-08 time=10:29:50 log_id=00091102 msg_id=0000000000145 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed wvs policy vulnscan1 from GUI(172.20.120.47) "</pre>

Related

- [00091101](#)
- [00091111](#)

00091111

Table 836:

Meaning
An administrator deleted a vulnerability scan policy.

Table 837:

Field name	Description
ID (log_id)	00091111 See “Log ID numbers” on page 23.

Table 838:

Example
<pre>date=2013-10-08 time=10:29:59 log_id=00091111 msg_id=000000000146 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted wvs policy vulnscan1 from GUI(172.20.120.47) "</pre>

Related

- [00091101](#)
- [00091102](#)

00093001

Table 839:

Meaning
An administrator created an anti-defacement monitor.

Table 840:

Field name	Description
ID (log_id)	00093001 See “Log ID numbers” on page 23.

Table 841:

Example
<pre>date=2013-10-08 time=10:17:38 log_id=00093001 msg_id=0000000000114 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added website 1 from GUI(172.20.120.47) "</pre>

Related

- [00093002](#)
- [00093011](#)

Table 842:

Meaning
An administrator changed an anti-defacement monitor.

Table 843:

Field name	Description
ID (log_id)	00093002 See “Log ID numbers” on page 23.

Table 844:

Example
<pre>date=2013-10-08 time=10:17:46 log_id=00093002 msg_id=000000000115 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed website 1 from GUI(172.20.120.47) "</pre>

Related

- [00093001](#)
- [00093011](#)

00093011

Table 845:

Meaning
An administrator deleted an anti-defacement monitor.

Table 846:

Field name	Description
ID (log_id)	00093011 See “Log ID numbers” on page 23.

Table 847:

Example
<pre>date=2013-10-08 time=10:17:56 log_id=00093011 msg_id=000000000116 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted website 1 from GUI(172.20.120.47) "</pre>

Related

- [00093001](#)
- [00093002](#)

Table 848:

Meaning
An administrator created an anti-defacement file filter.

Table 849:

Field name	Description
ID (log_id)	00093501 See “Log ID numbers” on page 23.

Table 850:

Example
<pre>date=2014-09-03 time=11:54:59 log_id=00093501 msg_id=000000003151 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added file-filter video_content from GUI(172.20.120.61) "</pre>

Related

- [00093502](#)
- [00093511](#)

Table 851:

Meaning
An administrator edited an anti-defacement file filter.

Table 852:

Field name	Description
ID (log_id)	00093502 See “Log ID numbers” on page 23.

Table 853:

Example
<pre>date=2014-09-10 time=17:06:02 log_id=00093502 msg_id=000085523288 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed file-filter video_files from GUI(172.22.14.6) "</pre>

Related

- [00093501](#)
- [00093511](#)

00093511

Table 854:

Meaning
An administrator deleted an anti-defacement file filter.

Table 855:

Field name	Description
ID (log_id)	00093511 See “Log ID numbers” on page 23.

Table 856:

Example
<pre>date=2014-09-03 time=12:15:06 log_id=00093511 msg_id=000000003152 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted file-filter video_content from GUI(172.20.120.61) "</pre>

Related

- [00093501](#)
- [00093502](#)

10000009

Table 857:

Meaning
An administrator powered on the FortiWeb appliance.

Table 858:

Field name	Description
ID (log_id)	10000009 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	information See “Priority level” on page 24.
Action (action)	start

Table 859:

Example
<pre>date=2013-10-08 time=01:33:34 log_id=10000009 msg_id=0000000000007 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="system" pri=information trigger_policy="" user=system ui=sys action=start status=success msg="FortiWeb started"</pre>

Related

- [Reboot, shut down, & boot up messages](#)
- [10000010](#)
- [10000011](#)

10000010

Table 860:

Meaning
A FortiWeb administrator rebooted the operating system of the appliance. If the administrator did this through the web UI, the log message includes the administrator's comment, if he or she provided one.

Table 861:

Field name	Description
ID (log_id)	10000010 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	critical See “Priority level” on page 24.
Action (action)	reboot

Table 862:

Example
<pre>date=2013-10-08 time=09:48:54 log_id=10000010 msg_id=00000000000070 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=reboot status=success msg="User admin rebooted the device from GUI(172.20.120.47).This is my comment."</pre>

Related

- [Reboot, shut down, & boot up messages](#)
- [10000009](#)
- [10000011](#)

10000011

Table 863:

Meaning
An administrator halted the operating system of the FortiWeb appliance in preparation to power off the hardware.

Table 864:

Field name	Description
ID (log_id)	10000011 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	notification See “Priority level” on page 24.
Action (action)	shutdown

Table 865:

Example
<code>date=2014-06-16 time=02:41:42 log_id=10000011 msg_id=000000022971 device_id=FVVM020000018466 vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=shutdown status=success msg="User admin shut down the device from GUI(172.22.6.241)."</code>

Related

- [Reboot, shut down, & boot up messages](#)
- [10000009](#)
- [10000010](#)

10000012

Table 866:

Meaning
An administrator's inactive session timed out.

Table 867:

Field name	Description
ID (log_id)	10000012 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	notification See “Priority level” on page 24.
Action (action)	shutdown

Table 868:

Example
<pre>date=2013-10-09 time=20:37:24 log_id=10000012 msg_id=0000000000340 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="system" pri=notification trigger_policy="" user=admin ui=console action=logout status=success msg="User admin time out on console"</pre>

Related

- [10000016](#)

10000013

Table 869:

Meaning
An administrator uploaded a data analytics definition file.

Table 870:

Field name	Description
ID (log_id)	10000013 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	information See “Priority level” on page 24.
Action (action)	update

Table 871:

Example
<pre>date=2014-04-10 time=13:01:33 log_id=10000013 msg_id=000044293782 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=information trigger_policy="" user=admin ui=GUI action=update status=success msg="User admin success loaded data analytics file from GUI(10.200.10.80)."</pre>

Table 872:

Meaning
An administrator deleted a locally-stored attack log, event log, or traffic log file.

Table 873:

Field name	Description
ID (log_id)	10000014 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	notice See “Priority level” on page 24.
User (user)	<administrator_name>
User Interface (ui)	{GUI(<mgmt_ip>) none telnet(<mgmt_ip>) ssh(<mgmt_ip>) console} Logins from jsconsole indicate use of the <i>CLI Console</i> widget on <i>System > Status > Status</i> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (action)	del
Status (status)	success
Message (msg)	User <administrator_name> has deleted disk log <file_str> from {GUI(<mgmt_ip>) none telnet(<mgmt_ip>) ssh(<mgmt_ip>) console}

Table 874:

Examples
date=2014-04-10 time=18:09:47 log_id=10000014 msg_id=000000195890 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=notice trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin has deleted disk log elog(2014-04-09-23:34:02).log from GUI(172.22.6.240)"

Related

- [00032006](#)

10000015

Table 875:

Meaning
A FortiWeb administrator downloaded a log file.

Table 876:

Field name	Description
ID (log_id)	10000015 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
User Interface (ui)	GUI
Action (action)	backup
Status (status)	success
Message (msg)	User <administrator_name> download {Attack Event Traffic } from GUI(<mgmt_ip>)

Table 877:

Example
<pre>date=2013-10-07 time=16:13:10 log_id=10000015 msg_id=000000001218 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=admin ui=GUI action=backup status=success msg="Successfully. User admin download Event LOG from GUI(172.20.120.47)."</pre>

Table 878:

Meaning
Either a FortiWeb administrator logged in successfully, or attempted to log in but failed.

Table 879:

Field name	Description
ID (log_id)	10000016 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	notification See “Priority level” on page 24.
User (user)	<administrator_name>
User Interface (ui)	{none telnet(<mgmt_ip>) ssh(<mgmt_ip>) console} Logins from jsconsole indicate use of the <i>CLI Console</i> widget on <i>System > Status > Status</i> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (action)	login
Status (status)	success
	failed
Message (msg)	User <administrator_name> logged in successfully from {(<mgmt_ip>) jsconsole telnet(<mgmt_ip>) ssh(<mgmt_ip>) }
	User <administrator_name> login failed from {(<mgmt_ip>) jsconsole telnet(<mgmt_ip>) ssh(<mgmt_ip>) }

Table 880:

Example
<pre>date=2014-04-10 time=13:31:37 log_id=10000016 msg_id=000044294845 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=notice trigger_policy="" user=admin ui=telnet action=login status=success msg="User admin logged in successfully from telnet(10.200.0.1) "</pre>

Related

- [10000012](#)

Table 881:

Meaning
Someone attempted to log in to a FortiWeb administrator account, but failed.

Table 882:

Solution
<p>If you suspect that an unauthorized person is attempting to log in to your FortiWeb, there are some preventative measures that you can take.</p> <ol style="list-style-type: none"> 1. Restrict physical access to the FortiWeb to ensure that only authorized persons can attach a console or computer to the appliance's local console port. 2. Configure all administrator accounts with trusted IPs that restrict login attempts to ones that originate only from your trusted, physically secured, private administrative network. Do not allow login attempts from hostile or untrusted IP addresses. If any administrator account uses a broad trusted IP definition such as 0.0.0.0/0.0.0.0, then due to that account, FortiWeb must allow login attempts from all IP addresses, including the Internet. Brute force login attempts are then a significant risk. 3. Enable strong password enforcement. Passwords must be significantly complex in length and character types in order to make brute force login attempts impractically slow. 4. Require regular password changes. 5. Enable only secure administrative protocols (SSH and HTTPS) on network interfaces. Insecure protocols such as HTTP and Telnet are easily susceptible to eavesdropping, man-in-the-middle, and other attacks that could compromise your connection, your password, or both.

Table 883:

Field name	Description
ID (log_id)	10000017 See “Log ID numbers” on page 23.
Sub Type (subtype)	admin See “Subtypes” on page 24.
Level (pri)	alert See “Priority level” on page 24.
User (user)	<administrator_name>
User Interface (ui)	{GUI(<mgmt_ip>) telnet(<mgmt_ip>) ssh(<mgmt_ip>) console}
Action (action)	login

Table 883:

Field name	Description
Status (status)	failure
Message (msg)	User <administrator_name> login failed from {GUI(<mgmt_ip>) telnet(<mgmt_ip>) ssh(<mgmt_ip>) console}

Table 884:

Example
<pre>date=2014-04-10 time=18:11:53 log_id=10000017 msg_id=000000195892 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=alert trigger_policy="" user=a ui=GUI action=login status=failed msg="User a login failed from GUI(172.22.6.240) "</pre>

Table 885:

Meaning
A FortiWeb administrator logged out.

Table 886:

Field name	Description
ID (log_id)	10000018 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	notification See “Priority level” on page 24.
User (user)	<administrator_name>
User Interface (ui)	{GUI(<mgmt_ip>) none telnet(<mgmt_ip>) ssh(<mgmt_ip>) console} Logins from jsconsole indicate use of the <i>CLI Console</i> widget on <i>System > Status > Status</i> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (action)	logout
Status (status)	success
Message (msg)	User <administrator_name> logout from {GUI(<mgmt_ip>) jsconsole telnet(<mgmt_ip>) ssh(<mgmt_ip>) console}

Table 887:

Example
date=2013-10-08 time=11:25:37 log_id=10000018 msg_id=0000000000272 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=admin ui=GUI action=logout status=success msg="User admin logs out from GUI(172.20.120.47)"

Related

- [10000012](#)

Table 888:

Meaning
A FortiWeb administrator upgraded the firmware image.

Table 889:

Field name	Description
ID (log_id)	10000019 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	critical See “Priority level” on page 24.
User (user)	<administrator_name>
User Interface (ui)	{GUI(<mgmt_ip>) none telnet(<mgmt_ip>) ssh(<mgmt_ip>) console} Logins from jsconsole indicate use of the <i>CLI Console</i> widget on <i>System > Status > Status</i> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (action)	upgrade
Status (status)	success
Message (msg)	User <administrator_name> upgrade the image from {GUI(<mgmt_ip>) jsconsole telnet(<mgmt_ip>) ssh(<mgmt_ip>) console}

Table 890:

Example
date=2014-04-10 time=15:26:51 log_id=10000019 msg_id=000000550016 device_id=FVVM040000018474 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=upgrade status=success msg="User admin upgrade the image from GUI(10.200.0.1) "

Related

- [10000020](#)

Table 891:

Meaning
A FortiWeb administrator downgraded the firmware image.

Table 892:

Field name	Description
ID (log_id)	10000020 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	critical See “Priority level” on page 24.
User (user)	<administrator_name>
User Interface (ui)	{GUI(<mgmt_ip>) none telnet(<mgmt_ip>) ssh(<mgmt_ip>) console} Logins from jsconsole indicate use of the <i>CLI Console</i> widget on <i>System > Status > Status</i> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (action)	downgrade
Status (status)	success
Message (msg)	User <administrator_name> downgraded the image from {GUI(<mgmt_ip>) jsconsole telnet(<mgmt_ip>) ssh(<mgmt_ip>) console}

Table 893:

Example
<pre>date=2014-04-10 time=15:22:38 log_id=10000020 msg_id=000000548987 device_id=FVVM040000018474 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=downgrade status=success msg="User admin downgraded the image from GUI(10.200.0.1)"</pre>

Related

- [10000019](#)

10000021

Table 894:

Meaning
A FortiWeb administrator restored the system configuration.

Table 895:

Field name	Description
ID (log_id)	10000021 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	critical See “Priority level” on page 24.
User (user)	<administrator_name>
User Interface (ui)	{GUI(<mgmt_ip>) none telnet(<mgmt_ip>) ssh(<mgmt_ip>) console} Logins from jsconsole indicate use of the <i>CLI Console</i> widget on <i>System > Status > Status</i> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (action)	restore
Status (status)	success
Message (msg)	User <administrator_name> downgraded the image from {GUI(<mgmt_ip>) jsconsole telnet(<mgmt_ip>) ssh(<mgmt_ip>) console}

Table 896:

Example
date=2014-08-06 time=18:37:45 log_id=10000021 msg_id=000016328576 device_id=FV-4KD3R13800048 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=restore status=success msg="User admin restored the configuration from GUI(172.22.6.149)"

Table 897:

Meaning
A FortiWeb administrator manually requested an update to either the FortiWeb regular virus database, the FortiWeb extended virus database, or the virus engine.

Table 898:

Field name	Description
ID (log_id)	10000022 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	critical See “Priority level” on page 24.
User (user)	<administrator_name>
User Interface (ui)	{GUI(<mgmt_ip>) none telnet(<mgmt_ip>) ssh(<mgmt_ip>) console} Logins from jsconsole indicate use of the <i>CLI Console</i> widget on <i>System > Status > Status</i> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (action)	update
Status (status)	success
Message (msg)	User<administrator_name> manually update {virus signature virus extend signature virus engine} from {GUI(<mgmt_ip>) jsconsole telnet(<mgmt_ip>) ssh(<mgmt_ip>) console} success

Table 899:

Example
date=2014-04-10 time=12:48:29 log_id=10000022 msg_id=000044292728 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=update status=success msg="User admin manually update virus signature from GUI(10.200.10.80) success"

Table 899:

```
date=2014-04-10 time=12:48:29 log_id=10000022 msg_id=000044292727
device_id=FV-1KD3A13800002 vd="root"
timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event
subtype="system" pri=critical trigger_policy="" user=admin ui=GUI
action=update status=success msg="User admin update virus extend
signature from GUI(10.200.10.80) success"
```

```
date=2014-04-10 time=12:48:29 log_id=10000022 msg_id=000044292726
device_id=FV-1KD3A13800002 vd="root"
timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event
subtype="system" pri=critical trigger_policy="" user=admin ui=GUI
action=update status=success msg="User admin update virus engine from
GUI(10.200.10.80) success"
```

Table 900:

Meaning
<p>One of the following events:</p> <ul style="list-style-type: none"> • A FortiWeb configuration backup to an FTP/SFTP server either succeeded or failed. • The scheduled configuration backup daemon started. Normally, this occurs at boot time. • An administrator downloaded a log file. • An administrator downloaded a backup of the system configuration file, fweb_system.conf. • An administrator downloaded an X.509 CSR.
Solution
<p>There could be several reasons why the backup failed.</p> <ol style="list-style-type: none"> 1. Check the IP address and login credentials that you have defined for FortiWeb's FTP/SFTP connection. 2. Verify that the directory you specified to receive backups exists, and has write permissions for that user name. 3. Make sure that the FTP/SFTP server's disk is not full, that it has enough disk space to receive the backup, and that that user name has not consumed its disk space quota, if any. 4. Verify that FortiWeb's system time is accurate. 5. Make sure that the backup is not scheduled during a network or server maintenance window, when the server or daemon are down. 6. Test that a reliable route exists between FortiWeb and the FTP/SFTP server by using <code>execute ping</code> and <code>execute traceroute</code> commands in the CLI. Keep in mind that if the network or the server was down for maintenance at the time of the backup attempt, the backup would have failed during that time, even if connectivity works for you now. 7. If you have firewalls or routers performing NAT between FortiWeb and the server, verify that FTP connections are allowed between them. Firewalls include host-based ones that may be on the server itself, such as Windows Firewall or <code>ipfw</code>. Keep in mind that the FTP protocol typically requires port 21, but that its mechanism style could be active or passive FTP, and that the protocol has both a command channel and a data transfer channel. If either of these channels fail, the backup will fail. SFTP typically requires port 22.

Table 901:

Field name	Description
ID (log_id)	10000023 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
User (user)	system

Table 901:

Field name	Description
User Interface (ui)	sys
Action (action)	backup
	start
Message (msg)	backup backup_<FTP-backup_name>_<timestamp_str> to <server_ipv4> <folder_str> {FAIL OK}

Table 902:

Examples
date=2013-10-08 time=09:42:19 log_id=10000023 msg_id=0000000000038 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="system" pri=notification trigger_policy="" user=system ui=sys action=backup status=failed msg="ftp backup backup_scheduled_backup_20131008094215 to ftp.example.com / FAILED"
date=2013-10-08 time=10:59:14 log_id=10000023 msg_id=000000146032 type=event subtype="system" pri=information device_id=FVVM020000003619 vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" user=system action=backup msg="backup backup_backup-to-ftp-server_20121113105913 to 172.20.120.225 Downloads/fortiweb/backups/ OK"
date=2013-10-05 time=19:26:12 log_id=10000023 msg_id=000000001038 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=system ui=sys action=start status=success msg="Backup daemon started"
date=2014-04-10 time=18:14:52 log_id=10000023 msg_id=000000195894 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=backup status=success msg="User admin backed up the Logging file from GUI(172.22.6.240) "
date=2014-04-10 time=18:17:06 log_id=10000023 msg_id=000000195895 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=backup status=success msg="User admin backed up the System config file from GUI(172.22.6.240) "
date=2014-04-10 time=18:18:05 log_id=10000023 msg_id=000000195897 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=backup status=success msg="User admin backed up the Local Cert(CSR) file from GUI(172.22.6.240) "

Related

- [11001008](#)

Table 903:

Meaning
A FortiWeb administrator changed the system time.

Table 904:

Field name	Description
ID (log_id)	10000027 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	critical See “Priority level” on page 24.
User (user)	<administrator_name>
User Interface (ui)	{GUI(<mgmt_ip>) none telnet(<mgmt_ip>) ssh(<mgmt_ip>) console} Logins from jsconsole indicate use of the <i>CLI Console</i> widget on <i>System > Status > Status</i> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (action)	change-time
Status (status)	success
Message (msg)	User <administrator_name> changed time from <date & time> to <date & time>.

Table 905:

Example
<pre>date=2014-04-10 time=15:13:20 log_id=10000027 msg_id=000044298000 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=console action=change-time status=failed msg="User admin changed time from Thu Apr 10 15:13:06 2014 to Thu Apr 10 15:13:20 2014 ."</pre>

Table 906:

Meaning
A FortiWeb administrator manually updated the IP reputation signature file.

Table 907:

Field name	Description
ID (log_id)	10000028 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	critical See “Priority level” on page 24.
User (user)	<administrator_name>
User Interface (ui)	{GUI(<mgmt_ip>) none telnet(<mgmt_ip>) ssh(<mgmt_ip>) console} Logins from jsconsole indicate use of the <i>CLI Console</i> widget on <i>System > Status > Status</i> in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (action)	update
Status (status)	success
Message (msg)	User <administrator_name> manually update IP Reputation signature from time from from {GUI(<mgmt_ip>) jsconsole telnet(<mgmt_ip>) ssh(<mgmt_ip>) console} success.

Table 908:

Example
date=2014-04-10 time=12:54:45 log_id=10000028 msg_id=000044293771 device_id=FV-1KD3A13800002 vd="root" timezone=" (GMT+8:00) Beijing, ChongQing, HongKong, Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=update status=success msg="User admin manually update IP Reputation signature from GUI(10.200.0.1) success"

Table 909:

Meaning
The logging daemon started. Normally, this occurs at boot time.

Table 910:

Field name	Description
ID (log_id)	11001008 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
User (user)	daemon
User Interface (ui)	daemon
Action (action)	start
Status (status)	success
Message (msg)	Log daemon started

Table 911:

Example
date=2013-10-05 time=19:26:02 log_id=11001008 msg_id=000000001037 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=daemon action=start status=success msg="Log daemon started"

Related

- [10000023](#)

Table 912:

Meaning
Someone attempted to log in to a web site where you have configured FortiWeb to provide end-user authentication, but failed.

Table 913:

Solution
<p>If you suspect that an unauthorized person is attempting to log in to your web site, there are some preventative measures that you can take.</p> <ol style="list-style-type: none"> 1. Require regular password changes. 2. Require strong passwords. Passwords must be significantly complex in length and character types in order to make brute force login attempts impractically slow. 3. Redirect requests for HTTP to a secure (HTTPS) URL. Insecure protocols such as HTTP are easily susceptible to eavesdropping, man-in-the-middle, and other attacks that could compromise your connection, your password, or both.

Table 914:

Field name	Description
ID (log_id)	11002003 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	alert See “Priority level” on page 24.
User (user)	daemon
User Interface (ui)	daemon
Action (action)	login
Status (status)	failed
Message (msg)	User <user_name> <auth-method_str> login failed from <source_ip_v4> request_url: <url>

Table 915:

Examples
<pre>date=2014-09-10 time=17:43:31 log_id=11002003 msg_id=000000852763 device_id=FV-3KD3R13800027 vd="Adomain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=alert trigger_policy="" user=daemon ui=daemon action=login status=failed msg="User test1 HTTP BASIC login failed from 10.0.6.25 request_url:fortinet.fortiweb.com/autotest/ldapuser.html"</pre>

Related

- [11002004](#)

Table 916:

Meaning
An end-user successfully logged in to a web site that you have configured FortiWeb to provide with authentication.

Table 917:

Field name	Description
ID (log_id)	11002004 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	information See “Priority level” on page 24.
User (user)	daemon
User Interface (ui)	daemon
Action (action)	login
Status (status)	success
Message (msg)	User <user_name> <auth-method_str> login successfully from <source_ipv4> request_url: <url>

Table 918:

Example
date=2014-09-10 time=17:43:39 log_id=11002004 msg_id=000000852769 device_id=FV-3KD3R13800027 vd="Adomain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=daemon action=login status=success msg="User test1 HTTP BASIC login successfully from 10.0.6.25 request_url:fortinet.fortiwab.com/autotest/ldapuser.html"

Related

- [11002003](#)

Table 919:

Meaning
FortiWeb has detected a change to a web site file that could indicate a defacement attack.

Table 920:

Field name	Description
ID (log_id)	11003601 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
User (user)	daemon
User Interface (ui)	daemon
Action (action)	monitor
Status (status)	success
Message (msg)	File <file_name> on site <site_name> has been changed. Please confirm or restore it.

Table 921:

Example
<pre>date=2014-04-10 time=14:43:11 log_id=11003601 msg_id=000044296936 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=monitor status=failed msg="File [/sig-db/signature.db] on site [2] has been changed. Please confirm or restore it."</pre>

Table 922:

Meaning
FortiWeb failed to connect to a web site that you have configured to be monitored by the anti-defacement feature. Therefore it could not determine whether or not the web site has been defaced.

Table 923:

Solution
<p>If anti-defacement could not connect to the web site:</p> <ol style="list-style-type: none"> 1. Verify the login and IP address that you provided. 2. On the web server, check the file system permissions for the account that FortiWeb is using to connect. (FortiWeb must be able to both read and, if it will be restoring files, write to the folder and files. 3. On Microsoft Windows, you may need to examine your security policy configuration to make sure that the account is authenticating as itself, and is not degrading to the guest account.) 4. Verify that a route exists between the FortiWeb and the web server, and that connectivity is reliable, with no packet loss. 5. Verify that any routers or firewalls between the appliance and the server, including Windows Firewall, are not blocking SSH, FTP, or CIFS connections. 6. Other troubleshooting varies by the protocol that FortiWeb is using to connect, such as checking for a compatible protocol version and cipher suite.

Table 924:

Field name	Description
ID (log_id)	11004002 See “Log ID numbers” on page 23.
Sub Type (subtype)	admin See “Subtypes” on page 24.
Level (pri)	warning See “Priority level” on page 24.
User Interface (ui)	anti-defacement
Action (action)	monitor

Table 924:

Field name	Description
Status (status)	alert
Message (msg)	Fail to connect to website <anti-defacement_name> (host is <server_ipv4>)

Table 925:

Example
<pre>date=2012-02-13 time=18:49:09 log_id=00032901 msg_id=000015400628 type=event subtype="admin" pri=warning device_id=FV-1KC3R086000008 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" ui=anti-defacement action=monitor status=alert reason=filechange msg="Fail to connect to website www.example.com (host is 10.0.0.1)"</pre>

Table 926:

Meaning
A failover occurred — that is, the secondary (standby) appliance in the FortiWeb high availability (HA) cluster assumed the duties of processing traffic because it detected that the primary (active) appliance had failed.

Table 927:

Field name	Description
ID (log_id)	11004601 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
User (user)	daemon
User Interface (ui)	daemon
Action (action)	HA-Switch
Status (status)	success
Message (msg)	HA switch from standby to main.

Table 928:

Example
<pre>date=2014-04-10 time=14:35:54 log_id=11004601 msg_id=000044296931 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=HA-Switch status=success msg="HA switch from standby to main."</pre>

Related

- [11004602](#)
- [11004603](#)
- [11004605](#)
- [11004606](#)
- [11004608](#)

Table 929:

Meaning
An administrator has manually synchronized configuration files from the active HA appliance to the standby appliance.

Table 930:

Field name	Description
ID (log_id)	11004602 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
User (user)	admin
User Interface (ui)	console
Action (action)	HA-Synchronize
Status (status)	success
Message (msg)	User admin synchronize the waf configuration to standby device from console.

Table 931:

Example
date=2014-04-10 time=14:55:59 log_id=11004602 msg_id=000044296940 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=information trigger_policy="" user=admin ui=console action=HA-Synchronize status=success msg="User admin synchronize the waf configuration to standby device from console."

Related

- [11004601](#)
- [11004603](#)
- [11004605](#)
- [11004606](#)
- [11004608](#)

Table 932:

Meaning
An appliance has been added to or removed from the high availability (HA) cluster.

Table 933:

Field name	Description
ID (log_id)	11004603 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
User (user)	daemon
User Interface (ui)	daemon
Action (action)	HA-member-left
Status (status)	success
Message (msg)	Member <device_id> {left join to the} HA group.

Table 934:

Example
<pre>date=2014-04-10 time=15:37:31 log_id=11004603 msg_id=000044298015 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=HA-member-left status=success msg="Member (FV-1KD3A13800001) left HA group."</pre>
<pre>date=2014-04-10 time=15:38:42 log_id=11004603 msg_id=000044298021 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=HA-member-join status=success msg="Member (FV-1KD3A13800001) join to the HA group."</pre>

Related

- [11004601](#)
- [11004602](#)
- [11004605](#)
- [11004606](#)
- [11004608](#)

Table 935:

Meaning
In a high availability (HA) cluster, the configuration has been restored from the active (master) to the standby (slave) appliance.

Table 936:

Field name	Description
ID (log_id)	11004605 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
User (user)	daemon
User Interface (ui)	daemon
Action (action)	restore
Status (status)	success
Message (msg)	HA restored the configuration from master : <device_id>

Table 937:

Example
<pre>date=2014-04-10 time=15:56:40 log_id=11004605 msg_id=000000187139 device_id=FV-1KD3A13800001 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=restore status=success msg="HA restored the configuration from master : FV-1KD3A13800002"</pre>

Related

- [11004601](#)
- [11004602](#)
- [11004603](#)
- [11004606](#)
- [11004608](#)

Table 938:

Meaning
In a high availability (HA) cluster, the firmware has been restored from the active (master) to the standby (slave) appliance.

Table 939:

Field name	Description
ID (log_id)	11004606 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
User (user)	daemon
User Interface (ui)	daemon
Action (action)	restore
Status (status)	success
Message (msg)	HA restored the image from master : <device_id>

Table 940:

Example
<pre>date=2014-04-10 time=16:49:38 log_id=11004606 msg_id=000000188232 device_id=FV-1KD3A13800001 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=restore status=success msg="HA restored the image from master : FV-1KD3A13800002"</pre>

Related

- [11004601](#)
- [11004602](#)
- [11004603](#)
- [11004605](#)
- [11004608](#)

Table 941:

Meaning
In a high availability (HA) cluster, the up/down status of the port that is monitored for link failure has changed.

Table 942:

Field name	Description
ID (log_id)	11004608 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
User (user)	daemon
User Interface (ui)	daemon
Action (action)	HA-monitor-port
Status (status)	success
Message (msg)	HA monitor port <port_name> status changed from down to up.

Table 943:

Example
<pre>date=2014-09-11 time=18:30:41 log_id=11004608 msg_id=000085524326 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=HA-monitor-port status=success msg="HA monitor port (port4) status changed from up to down."</pre>
<pre>date=2014-09-11 time=18:30:35 log_id=11004608 msg_id=000085524325 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=HA-monitor-port status=success msg="HA monitor port (port4) status changed from down to up."</pre>

Related

- [11004601](#)
- [11004602](#)
- [11004603](#)
- [11004605](#)
- [11004606](#)

Table 944:

Meaning
<p>Either:</p> <ul style="list-style-type: none"> the FortiGuard Antivirus, FortiGuard FortiWeb Security Service, or FortiGuard IP Reputation Intelligence Service (IRIS) license could not be authenticated the FortiGuard services were up-to-date as of the time when FortiWeb polled FortiGuard for updates FortiWeb could not connect to the FDN update servers, or the connection was interrupted, and therefore could not update its packages for FortiGuard services a FortiGuard service update installation failed a FortiGuard service update succeeded License authentication determined that the FortiWeb-VM license uploaded by an administrator is either valid or invalid.
Solution
<p>If a FortiGuard license could not be authenticated:</p> <ol style="list-style-type: none"> 1. Check with the Fortinet Technical Support web site to make sure that you have purchased a license for this FortiWeb. If you have an HA pair, you should have one license for each appliance in the pair. 2. Verify that the license is not currently expired, or not yet in effect. 3. Verify that FortiWeb can connect to the Internet to validate its license. To do this, it will require a valid route, DNS settings, and possibly also time settings. If connectivity is unreliable, the initial license request may fail. In this case, you can either wait 30 minutes for the appliance to request authorization again, or use the CLI command <code>execute update-now</code> to force an immediate license authentication query. <p>If FortiWeb could not connect to the FDN or package retrieval failed, verify that FortiWeb has reliable Internet connectivity.</p> <p>If the license is invalid:</p> <ol style="list-style-type: none"> 1. Check with the Fortinet Technical Support web site to make sure that you have purchased a license for this FortiWeb. If you have an HA pair, you should have one license for each appliance in the pair. If you are using a trial license, verify that the trial period has not expired. 2. If you are using a purchased license, verify that you have uploaded the license file to FortiWeb-VM. 3. Verify that the license has not been already used by another. (If you upload the license and it is currently associated with a different management IP, the web UI will display an error message: <code>Duplicate license detected.</code>) 4. Verify that the number of allocated vCPUs does not exceed the limit of the license. <p>Verify that FortiWeb can connect to the Internet to validate its license. To do this, it will require a valid route, DNS settings, and possibly also time settings. If connectivity is unreliable, the initial license request may fail. In this case, you can either wait 30 minutes for the appliance to request authorization again, or use the CLI command <code>execute update-now</code> to force an immediate license authentication query.</p>

Table 945:

Field name	Description
ID (log_id)	11005901 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	error (for unauthorized licenses, update failures, or connectivity errors) information (for up-to-date results from the FortiGuard poll) critical (for invalid license) See “Priority level” on page 24.
Message (msg)	Fortiweb {ip intelligence signature virus engine virus extend signature virus signature waf signature} is unauthorized
	Fortiweb {ip intelligence signature virus engine virus extend signature virus signature waf signature} is already up-to-date
	update failed, failed to connect to fds server!
	update failed, couldn't receive a update package!
	Fortiweb {ip intelligence signature virus engine virus extend signature virus signature waf signature} update failed
	Fortiweb {ip intelligence signature virus engine virus extend signature virus signature waf signature} update succeeded
	License status changed to {VALID INVALID}

Table 946:

Examples
<pre>date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000195866 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb virus engine is unauthorized"</pre>
<pre>date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000123728 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=error trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb virus extend signature is unauthorized"</pre>

Table 946:

<p>date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000123727 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi" type=event subtype="system" pri=error trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb virus signature is unauthorized"</p>
<p>date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000146653 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb waf signature is already up-to-date"</p>
<p>Fortiweb waf signature is unauthorized date=2014-04-10 time=16:00:02 log_id=11005901 msg_id=000000734617 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="system" pri=critical trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb waf signature is unauthorized"</p>
<p>date=2014-04-10 time=16:00:02 log_id=11005901 msg_id=000000734621 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=event subtype="system" pri=critical trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb ip intelligence signature is unauthorized"</p>
<p>date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000189416 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb ip reputation signature is already up-to-date"</p>
<p>date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000158889 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi" type=event subtype="system" pri=error trigger_policy="" user=daemon ui=daemon action=update status=failed msg="update failed failed to connect fds server!"</p>
<p>date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000070564 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi" type=event subtype="system" pri=error trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb virus extend signature update failed"</p>
<p>date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000068286 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb virus engine update succeeded"</p>

Table 946:

```
date=2014-04-10 time=09:36:15 log_id=11005901 msg_id=000000022248
device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00)Pacific
Time(US&Canada)" type=event subtype="system" pri=critical
trigger_policy="" user=daemon ui=daemon action=update status=failed
msg="License status changed to VALID"
```

```
date=2014-04-10 time=09:36:15 log_id=11005901 msg_id=0000000104120
device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00)Pacific
Time(US&Canada)" type=event subtype="system" pri=critical
trigger_policy="" user=daemon ui=daemon action=update status=failed
msg="License status changed to INVALID"
```

Table 947:

Meaning
A FortiWeb administrator brought up or brought down a network interface.

Table 948:

Field name	Description
ID (log_id)	11006004 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	information See “Priority level” on page 24.
User (user)	daemon
User Interface (ui)	none
Action (action)	check-resource
Status (status)	failed
Message (msg)	interface <interface_name> link {up down}

Table 949:

Examples
<pre>date=2013-10-08 time=09:48:12 log_id=11006004 msg_id=0000000000068 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=none action=check-resource status=failed msg="interface port2 link up"</pre>
<pre>date=2013-10-08 time=14:09:10 log_id=11006004 msg_id=0000000000286 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=none action=check-resource status=failed msg="interface vlan3 link down"</pre>

Related

- [00004401](#)
- [00004402](#)
- [00004411](#)

Table 950:

Meaning
<p>Either the CPU usage:</p> <ul style="list-style-type: none"> became too high and exceeded the alert threshold, or lowered until it did not exceed the alert threshold anymore

Table 951:

Field name	Description
ID (log_id)	11006005 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
User (user)	daemon
User Interface (ui)	none
Action (action)	check-resource
Status (status)	failed
Message (msg)	CPU usage raise too high,CPU(<percentage_int>)
	CPU usage reduced,CPU(<percentage_int>)

Table 952:

Examples
<pre>date=2013-10-05 time=20:26:59 log_id=11006005 msg_id=000000001043 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=none action=check-resource status=failed msg="CPU usage raise too high,CPU(96)"</pre>
<pre>date=2013-10-07 time=15:29:35 log_id=11006005 msg_id=000000001207 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=none action=check-resource status=failed msg="CPU usage reduced, CPU usage is 53"</pre>

Related

- [00032006](#)
- [11006006](#)

Table 953:

Meaning
<p>Either the RAM usage:</p> <ul style="list-style-type: none"> became too high and exceeded the alert threshold, or lowered until it did not exceed the alert threshold anymore

Table 954:

Field name	Description
ID (log_id)	11006006 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
User (user)	daemon
User Interface (ui)	none
Action (action)	check-resource
Status (status)	failed
Message (msg)	mem usage raise too high,mem(<usage_int>)
	mem usage reduced,mem(<usage_int>)

Table 955:

Examples
<pre>date=2013-10-05 time=20:26:59 log_id=11006006 msg_id=000000001042 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=none action=check-resource status=failed msg="mem usage raise too high,mem(96) "</pre>
<pre>date=2013-10-05 time=20:29:06 log_id=11006006 msg_id=000000001048 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=none action=check-resource status=failed msg="mem usage reduced,mem(52) "</pre>

Related

- [00032006](#)
- [11006005](#)

Table 956:

Meaning
A certificate revocation list (CRL) has been updated using a query to a server.

Table 957:

Field name	Description
ID (log_id)	11006701 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	notice See “Priority level” on page 24.
User (user)	system
User Interface (ui)	none
Action (action)	edit
Status (status)	success
Message (msg)	A CRL is updated crl=<crl_name> method=HTTP

Table 958:

Examples
<pre>date=2014-04-10 time=17:14:18 log_id=11006701 msg_id=000000179557 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=notice trigger_policy="" user=system ui=none action=edit status=success msg=" A CRL is updated crl=CRL_4 method=HTTP"</pre>

Related

- [00008801](#)
- [00008811](#)
- [00009301](#)
- [00009311](#)

Table 959:

Meaning
A web server that belongs to a server pool definition became available (up) or unavailable (down) according to the configured server health check, if any.
Solution
<p>If a web server is being detected as unavailable, but it is actually up:</p> <ol style="list-style-type: none"> 1. Verify that you have selected a server health check in the server pool definition. 2. Verify that the server health check is using a method to contact the server that the server can respond to. If you are using <i>Ping</i>, for example, the server must be responsive to ICMP ECHO_REQUEST signals.

Table 960:

Field name	Description
ID (log_id)	19999496 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	alert See “Priority level” on page 24.
Message (msg)	policy <policy_name> Physical Server[<pserver_name>:<pserver-port_int>] is {down up}

Table 961:

Examples
<pre>date=2013-10-07 time=12:27:45 log_id=19999496 msg_id=000000001136 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="system" pri=alert trigger_policy="" user=daemon ui=daemon action=check-resource status=failed msg="policy policy1 Physical Server[apache1:80] is up"</pre>
<pre>date=2013-10-05 time=19:26:44 log_id=19999496 msg_id=000000001039 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=event subtype="system" pri=alert trigger_policy="" user=daemon ui=daemon action=check-resource status=failed msg="policy policy1 Physical Server[apache1:80] is down"</pre>

Related

- [00040001](#)
- [00040002](#)
- [00040011](#)

Table 962:

Meaning
The number of concurrent sessions has been reduced. For more information on model- or configuration-dependent limits, see the FortiWeb Administration Guide .

Table 963:

Field name	Description
ID (log_id)	19999497 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	alert See “Priority level” on page 24.
Message (msg)	policy <policy_name> concurrent session reduced

Table 964:

Examples
date=2014-04-10 time=18:04:19 log_id=19999497 msg_id=000044306075 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=alert trigger_policy="" user=daemon ui=daemon action=none status=failed msg="policy test concurrent session reduced"

Related

- [19999498](#)

Table 965:

Meaning
The maximum number of concurrent sessions has been reached. For more information on model- or configuration-dependent limits, see the FortiWeb Administration Guide .

Table 966:

Field name	Description
ID (log_id)	19999498 See “Log ID numbers” on page 23.
Sub Type (subtype)	system See “Subtypes” on page 24.
Level (pri)	alert See “Priority level” on page 24.
Message (msg)	policy <policy_name> concurrent session exceed threshold

Table 967:

Examples
date=2014-04-10 time=18:03:39 log_id=19999498 msg_id=000044305882 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi" type=event subtype="system" pri=alert trigger_policy="" user=daemon ui=daemon action=check-resource status=failed msg="policy test concurrent session exceed threshold"

Related

- [19999497](#)

Attack

Attack log messages record traffic that violated its matching policy. Log ID numbers of this type are listed in [Table 968](#).

The operating mode, network topology, and the rule's configured *Action* can all affect how a policy responds to an attack, data leak, or server information disclosure. Depending on your configuration, violating traffic is either:

- blocked
- sanitized, then passed through
- allowed to continue unmodified (that is, logged only)

FortiWeb does not record the following types of attack logs individually. Instead, it records them periodically while the attack is ongoing, even if the attack has multiple sources:

- DoS attacks
- Padding oracle attacks
- HTTP/HTTPS protocol constraints

This aggregation prevents FortiWeb from flooding attack logs with identical or very similar messages. To differentiate logs caused by individual attacks from those caused by multiple attacks in the same category, FortiWeb records whether it generated the attack log message after matching multiple signatures.

In the attack log, the message field of aggregated log messages displays the message `rule_name : Custom Access Violation`.

In aggregated attacks log, the type field displays the message `Multiple Custom access rule Violations`.

To locate a description for an attack log message, match the *ID* (`log_id`) field in the attack log message with that shown in [Table 968](#). All attack log messages have the same body fields, described in [“Attack log fields” on page 380](#).

For attack log messages generated by a HTTP protocol constraint, the associated policy name is displayed in the raw view (`[policy_name:<protocol_constraint_name>]`) but not in the formatted view.

Table 968:Attack logs by subtype & ID

ID (log_id)	Sub Type (subtype)	Message (msg)
20000001	waf_allow_method	HTTP Method Violation
20000002	allow_host	HTTP Host Violation
20000003	waf_page_rule	Page Access Rule Violation
20000004	waf_start_page	Start Page Violation
20000005	waf_cookie_poison	cookie name (<parameter_name>) : Cookie Poisoning [<original_value> -> <corrupted_value>; Domain: <domain>; Path: <path>
20000006	waf_parameter_rule	Parameter Validation Violation: (<parameter_name>)

Table 968:Attack logs by subtype & ID

ID (log_id)	Sub Type (subtype)	Message (msg)
20000007	waf_black_ip	Blacklisted IP blocked
20000008	waf_url_access	<rule_name> : URL Access Violation
20000009	waf_custom_signature_match	Custom Signature Detection: <custom_signature_rule_name>
20000010 waf_signature_detection		Credit Card Detection : Signature ID n
		Cross Site Scripting : Signature ID n
		Cross Site Scripting(Extended) : Signature ID n
		Generic Attacks- <subtype_name> : Signature ID n
		Generic Attacks(Extended)- <subtype_name> : Signature ID n
		Information Disclosure- <subtype_name> : Signature ID n
		KnownExploits- <subtype_name> : Signature ID n
		SQL Injection : Signature ID n where n is the index number of the specific predefined attack or data leak signature
		SQL Injection(Extended) : Signature ID n
		Bad Robot : Signature ID n
		Trojans : Signature ID n
20000019	waf_hidden_fields	Hidden Field Manipulation
20000018	waf_brute_login	Brute Force Login Violation
20000030	waf_custom_access	<custom_rule_name> : Custom Access Violation
20000032	waf_header_overflow	[policy_name: <protocol_constraint_name>] :Header Length Exceeded: (the current header length n exceeded the maximum header length limitation n)

Table 968:Attack logs by subtype & ID

ID (log_id)	Sub Type (subtype)	Message (msg)
20000033	waf_headline_overflow	[policy_name:<protocol_constraint_name>] :Header Line Length Exceeded: (the current HTTP header line length <i>n</i> exceeded the maximum length limitation <i>n</i>)
20000034	waf_body_overflow	[policy_name:<protocol_constraint_name>] :Body Length Exceeded: (the current HTTP body length <i>n</i> exceeded the maximum HTTP body length limitation <i>n</i>)
20000035	waf_content_overflow	[policy_name:<protocol_constraint_name>] : Content Length Exceeded: (the current content length <i>n</i> exceeded the maximum content length limitation <i>n</i>)
20000036	waf_parameter_overflow	[policy_name:<protocol_constraint_name>] : Total URL and Body Parameters Length Exceeded: (the current URL and body length <i>n</i> exceeded the maximum length limitation <i>n</i>)
20000037	waf_request_overflow	[policy_name:<protocol_constraint_name>] : HTTP Request Length Exceeded: (the current request length <i>n</i> exceeded the maximum request length limitation <i>n</i>)
20000038	waf_url_parameter_overflow	[policy_name:<protocol_constraint_name>] : Total URL Parameters Length Exceeded: (the current URL parameter length <i>n</i> exceeded the maximum length limitation <i>n</i>)
20000039	waf_illegal_http_version	[policy_name:<protocol_constraint_name>] : Illegal HTTP Version
20000040	waf_cookiecount_overflow	[policy_name:<protocol_constraint_name>] : Too Many Cookies in Request: (cookie number <i>n</i> exceeded the maximum cookie number limitation <i>n</i>)
20000041	waf_req_headline_overflow	[policy_name:<protocol_constraint_name>] : Too Many Headers In Request: (header line number <i>n</i> exceeded the maximum header line number limitation <i>n</i>)

Table 968:Attack logs by subtype & ID

ID (log_id)	Sub Type (subtype)	Message (msg)
20000042	waf_ip_reputation	IP Reputation Violation: <category_name>
20000043	waf_url_parameter_count_overflow	[policy_name: <protocol_constraint_name>] : Too Many Parameters in Request: (the current parameter number n exceeded the maximum parameter number limitation n)
20000044	waf_illegal_hostname	[policy_name: <protocol_constraint_name>] : Illegal Host Name: (host name <host> is illegal)
20000045	waf_illegal_file_type	filename [<file_str>]: Illegal file size/type
20000046 (when based upon the HTTP session ID)	DDOS based on HTTP session: waf_http_request_overflow	DoS Attack: HTTP Flood Prevention Violation
20000047 (when based upon the source IP)	DDOS based on HTTP session: waf_tcp_connection_overflow	DoS Attack: Malicious IPs Violation
20000048	waf_max_num_ranges_in_Range_header	[policy_name: <protocol_constraint_name>] : Too Many Range Headers: (the range header number n exceeded the maximum range header number n)
20000049	http_protocol_error	[policy_name: <protocol_constraint_name>] : Malformed Request - Header Too Large : Malformed Request or [policy_name: <protocol_constraint_name>] : Malformed Request - Parameter Too Large : Malformed Request
20000050 (when based upon the HTTP session ID)	DDOS based on source IP: waf_http_request_overflow	DoS Attack: HTTP Access Limit Violation

Table 968:Attack logs by subtype & ID

ID (log_id)	Sub Type (subtype)	Message (msg)
20000051 (when based upon the source IP)	DDOS based on source IP: waf_tcp_connection_overflow	DoS Attack: TCP Flood Prevention Violation
20000052	https_connection_failed	Varies by the cause of the SSL/TLS error. See “SSL/TLS error messages” on page 383.
20000053	waf_padding_oracle	Padding Oracle Attack
21000022	waf_dos_prevention_type	DoS Attack: SYN Flood
		DoS Attack: SYN Flood

Attack log fields

Fields in the body of attack log messages are described below.

For descriptions of header fields that exist in every log message, see [“Header & body fields” on page 15.](#)

Meaning
Traffic violating a policy was detected by the FortiWeb appliance.

Solution	
<p>If your appliance was:</p> <ul style="list-style-type: none"> operating in reverse proxy or true transparent proxy mode and configured to deny traffic (e.g. the <i>Action</i> is <i>Alert & Deny</i> in the log message) <p>the traffic was blocked. No action is required. If many attacks come from a client, though, for performance reasons, consider blacklisting its IP address.</p> <p>Otherwise, if your appliance was:</p> <ul style="list-style-type: none"> operating in offline protection or transparent inspection mode or configured only to monitor traffic (e.g. <i>Monitor Mode</i> was enabled or the <i>Action</i> is <i>Alert</i>, not <i>Alert & Deny</i>) <p>examine the web server to determine whether or not it was affected.</p> <p>By the nature of log-only actions, detected attack attempts are logged but not blocked. You may also want to determine if the attack is from a single source IP address or distributed: blacklisting an offending client may help you to efficiently prevent further attack attempts, improving performance, until you can take further action.</p> <p>By the nature of the network topology for offline protection mode (which can potentially cause differences in speeds of the separate routing paths), and asynchronous inspection for transparent inspection mode, blocking cannot be guaranteed. For details, see the FortiWeb Administration Guide.</p> <p>Tip: If an attack is not being detected as you expect, enable session management, traffic logging, and packet payload retention. You can examine the traffic log's packet payload to determine why it is not matching your profile rules and/or enabled attack signatures. For instructions, see the FortiWeb Administration Guide.</p>	
Field name	Description
ID (log_id)	An identifying number. See “Log ID numbers” on page 23 and the column “ID” on page 376.
Sub Type (subtype)	See “Subtypes” on page 24 and the column “Sub Type” on page 376.
Level (pri)	alert
Action (action)	<p>The action that you configured FortiWeb to take in response to the policy violation, such as:</p> <p>Alert</p> <p>or</p> <p>Alert_Deny</p> <p>Action options vary by the nature of the attack. For details on actions, see the FortiWeb Administration Guide.</p>
Service (service)	<service_name>
Policy (policy)	<server-policy_name>
Method (http_method)	Varies by the web application, but is usually GET or POST.

Field name	Description
HTTP Host (http_host)	The domain name as it appears in the request from the client. This name can be different from your internal DNS name, if any, for the web server, or, if you are using HTTP Host : rewrites, different from the domain name of the virtual host on the web server. (For example, www.example.co.jp instead of www1.local or the virtual host that serves responses for all DNS names, www.example.com.)
URL (http_url)	The URL as it appears in the request from the client. Can be a rewritten URL. This URL does not include the service or host name (for example, /main/index.html).
User Agent (http_agent)	The HTTP client platform, as it is reported by the client itself. This is often fake in attacks.
HTTP Session ID (http_session_id)	The HTTP session identifier associated with the HTTP request (if any). The ID may be <code>unknown</code> if the Session Management option is not enabled in the governing protection profile.
Message (msg)	See “Message” on page 376 .
Signature Subclass (signature_subclass)	The name of the signature subclass. If the current signature has no subclass, the main class is displayed.
Signature ID (signature_id)	The ID of the specific signature within the subclass that triggered the log message.
Source Country (srccountry)	The country that is the source of the traffic.
HTTP Content Routing (content_switch_name)	The name of the associated HTTP content routing policy.
Server Pool (server_pool_name)	The name of the server pool in the associated server policy.
Example	
<pre>date=2014-06-22 time=23:52:38 log_id=20000010 msg_id=000000102972 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT-8:00) Pacific Time (US&Canada)" type=attack subtype="waf_signature_detection" pri=alert trigger_policy="" severity_level=Low proto=tcp service=http action=Alert policy="Auto-policy" src=10.0.8.103 src_port=1114 dst=10.20.8.22 dst_port=80 http_method=get http_url="/" http_host="10.0.8.22" http_agent="Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; " http_session_id=none msg="[Signatures name: FWB_server_protection] [main class name: Information Disclosure] [sub class name: HTTP Header Leakage]: 080200004" signature_subclass="HTTP Header Leakage" signature_id="080200004" srccountry="Reserved" content_switch_name="none" server_pool_name="Auto-ServerFarm"</pre>	

SSL/TLS error messages

If you are configuring HTTPS for the first time, and there are configuration errors still, you might see some SSL or TLS-related error messages. Because they are rare and tend to indicate a potential attack attempt, they are located in the attack logs, except for cipher or key exchange errors, which tend to be traffic flow problems (see [“Traffic” on page 386](#)).

Although the *ID* (*log_id*) is the same for all HTTPS connection errors (20000052), the *Message* (*msg*) field varies by the cause.

Table 969:HTTPS attack log messages

Message (msg)	Cause & description
X509 Error 2 - Unable to get issuer certificate	The CA's certificate does not exist in the store of trusted CAs (<i>System > Certificates > CA</i>), nor is it included in a signing chain within the certificate file.
X509 Error 3 - Unable to get certificate CRL	Unable to get certificate CRL. The CRL of a certificate could not be found. Unused.
X509 Error 4 - The certificate signature could not be decrypted.	The certificate's signature value could not be determined, and therefore it could not be decrypted. It does not mean that the signature did not match the expected value. This applies only to RSA keys.
X509 Error 5 - The CRL signature could not be decrypted	Unable to decrypt CRL's signature the CRL signature could not be decrypted: this means that the actual signature value could not be determined rather than it not matching the expected value. Unused.
X509 Error 6 - Unable to decode issuer public key	The public key in the certificate's CA's Subject Public Key Info: field could not be read.
X509 Error 7 - Certificate signature failure	The certificate's signature is invalid.
X509 Error 8 - CRL signature failure	The signature of the certificate in the CRL is invalid. Unused.
X509 Error 9 - Certificate is not yet valid	The certificate's Not Before: field is after the current time and date.
X509 Error 10 - Certificate has expired	The certificate's Not After: field is after the current time and date.
X509 Error 11 - CRL is not yet valid	CRL is not yet valid the CRL is not yet valid. Unused.
X509 Error 12 - CRL has expired	CRL has expired the CRL has expired. Unused.
X509 Error 13 - Format error. The certificate notBefore field contains an invalid time	The certificate's Not Before: field contains an invalid time.

Table 969:HTTPS attack log messages

Message (msg)	Cause & description
X509 Error 14 - Format error. The certificate notAfter field contains an invalid time	The certificate's <code>Not After:</code> field contains an invalid time.
X509 Error 15 - Format error. The CRL lastUpdate field contains an invalid time	Format error in URL's <code>lastUpdate</code> field. The CRL <code>lastUpdate</code> field contains an invalid time. Unused.
X509 Error 16 - Format error. The CRL nextUpdate field contains an invalid time	Format error in CRL's <code>nextUpdate</code> field. The CRL <code>nextUpdate</code> field contains an invalid time. Unused.
X509 Error 17 - An error occurred trying to allocate memory	FortiWeb is out of memory. This should never happen.
X509 Error 18 - Certificate is self signed and the same certificate cannot be found in the list of trusted certificates	The certificate is self-signed meaning that it is acting as its own CA. However, the certificate does not exist in the store of trusted CAs (<i>System > Certificates > CA</i>).
X509 Error 19 – Root certificate could not be found locally	The certificate contains a signing chain that is not complete. The certificate's signing chain must terminate with the certificate of a CA that is trusted by FortiWeb (<i>System > Certificates > CA</i>).
X509 Error 20 - Issuer certificate could not be found	The certificate indicates an <code>Issuer:</code> field (CA), so it should not be self-signed. However, the certificate's signing chain does not contain that issuing CA's certificate.
X509 Error 21 - No signatures could be verified. Chain contains only one certificate and it is not self signed	The certificate's signing chain contains only one certificate. However, the certificate is not a self-signed certificate.
X509 Error 22 - Certificate chain too long	The certificate chain length is greater than the supplied maximum depth. Unused.
X509 Error 23 - The certificate has been revoked	The certificate has been revoked. Unused.
X509 Error 24 - Invalid CA certificate	Either the CA's certificate is not actually from a CA, or its extensions are not consistent with the supplied purpose.
X509 Error 25 - Path length constraint exceeded	The certificate's <code>Basic Constraints:</code> field's <code>Path Length Constraint=</code> parameter was exceeded.

Table 969:HTTPS attack log messages

Message (msg)	Cause & description
X509 Error 26 - Unsupported certificate	The certificate's <code>Key Usage</code> : field or <code>Enhanced Key Usage</code> : field does not match FortiWeb's purpose. This could occur if, for example, an email signing certificate were to be accidentally used as a server certificate.
X509 Error 27 - Certificate not trusted	The root CA's certificate is not marked as trusted for the certificate's purpose (<code>Certificate Usage</code> : field).
X509 Error 28 - Certificate rejected.	The root CA's certificate is marked to reject the certificate's purpose (<code>Certificate Usage</code> : field).
X509 Error 29 - Subject issuer mismatch	The current candidate issuer certificate was rejected because its <code>Subject</code> : name did not match the <code>Issuer</code> : name of the current certificate. Only displayed when the <code>-issuer_checks</code> option is set.
X509 Error 30 - Authority and subject key identifier mismatch	The current candidate issuer certificate was rejected because its <code>Subject Key Identifier</code> : was present and did not match the <code>Authority Key Identifier</code> : current certificate. Only displayed when the <code>-issuer_checks</code> option is set.
X509 Error 31 - Authority and issuer serial number mismatch	The current candidate issuer certificate was rejected because its <code>Issuer</code> : name and <code>Serial Number</code> : field was present and did not match the <code>Authority Key Identifier</code> : of the current certificate. Only displayed when the <code>-issuer_checks</code> option is set.
X509 Error 32 - Key usage does not include certificate signing	The certificate of the CA currently being examined in the signing chain was rejected because its <code>Key Usage</code> : extension does not permit certificate signing.
X509 Error 50 - Application verification failure	Application verification failure an application specific error. Unused.
X509 Error 52 - Get client certificate failed	FortiWeb does not have the certificate of the CA that signed the personal certificate in its store of trusted CAs (<code>System > Certificates > CA</code>), and therefore cannot verify the personal certificate.
X509 Error 53 - Protocol error	The client did not present its personal certificate to FortiWeb. This could be caused by the client not having its personal certificate properly installed.

Traffic

Traffic log messages record requests that a FortiWeb policy accepted or blocked. If the request was successful, it also includes the reply. Each log message represents its whole HTTP transaction.

Traffic logs do **not** record non-HTTP/HTTPS traffic such as FTP. This type of traffic is forwarded to your web servers if you have enabled IP-layer forwarding.

Traffic log messages are described below. For descriptions of header fields not mentioned here, see [“Header & body fields” on page 15](#).

Table 970:

Meaning
Traffic matching and complying with a policy passed through or by FortiWeb. If there is an error in the message, however, and the request/response used HTTPS, FortiWeb could not scan it. Depending on the mode of operation, an attack could have bypassed FortiWeb.

Table 971:

Solution
<p>Reponse times can often be improved, for example, by regular expression tuning, offloading SSL/TLS from your back-end server to your FortiWeb (especially if the model supports hardware acceleration), and/or offloading compression. For performance tips, see the FortiWeb Administration Guide.</p> <p>If HTTPS traffic is not flowing as you expect or not being inspected, and you have recently enabled HTTPS, typically this is due to a misconfiguration. The error message in the <code>msg</code> field will indicate the appropriate solution:</p> <ul style="list-style-type: none"> • <code>No Server Certificate for SSL Connection</code> — FortiWeb does not have the server certificate, so it cannot decode the SSL traffic. To fix this, upload the web server's certificate to FortiWeb. • <code>SSL Certificate Key Mismatch</code> — An X.509 server certificate was uploaded to FortiWeb, but its private key did not match the one used by this HTTPS session. To fix this, upload the back-end web server's current certificate. • <code>Ephemeral keys cannot be decrypted</code> — Ephemeral Diffie-Hellman key exchange can't be inspected due to the property of perfect forward secrecy, which makes real-time HTTPS inspection impossible. To fix this, disable ephemeral Diffie-Hellman on the back-end web server, and select a different key exchange method. • <code>Unsupported Cipher for SSL Connection</code> — Either message digest (MAC) authentication failed or the MAC did not exist, or the transaction used an unsupported cipher suite. To fix this, on the back-end web server, disable cipher suites that are not supported by FortiWeb. • <code>Unmonitored SSL Connection</code> — The HTTPS session was initiated before FortiWeb was deployed or before the server policy was enabled, so FortiWeb could not listen for the key exchange, and therefore cannot decrypt subsequent requests/responses in this HTTPS session. To fix this, on the back-end web server, clear HTTPS sessions and force clients to renegotiate. <p>If your appliance was operating in reverse proxy or true transparent proxy mode, the traffic was blocked, and no attack could have passed through to your protected web servers. No action is required except to make sure that you have uploaded to FortiWeb the correct certificate for all protected web servers.</p> <p>Otherwise, if your appliance was:</p> <ul style="list-style-type: none"> • operating in offline protection or transparent inspection mode or • configured only to monitor traffic (e.g. <i>Monitor Mode</i> was enabled or the <i>Action</i> is <i>Alert</i>, not <i>Alert & Deny</i>) <p>examine the web server to determine whether or not an encrypted attack has passed through. You should also examine your web server's HTTPS configuration and disable cipher suites and key exchanges that are not supported by FortiWeb so that during negotiation with clients, your web server does not agree to use encryption that FortiWeb cannot scan for attacks.</p> <p>By the nature of log-only actions, detected attack attempts are logged but not blocked. You may also want to determine if the attack is from a single source IP address or distributed: blacklisting an offending client may help you to efficiently prevent further attack attempts, improving performance, until you can take further action.</p> <p>By the nature of the network topology for offline protection mode (which can potentially cause differences in speeds of the separate routing paths), and asynchronous inspection for transparent inspection mode, blocking cannot be guaranteed and some key exchanges are not supported. For details, see the FortiWeb Administration Guide.</p>

Table 972:

Field name	Description
ID (log_id)	30000000 All traffic log messages share the same ID (log_id=30000000). See “Log ID numbers” on page 23 .
Sub Type (subtype)	http All traffic log messages share the same subtype (subtype=http). See “Subtypes” on page 24 .
Level (pri)	notification See “Priority level” on page 24 .
Message (msg)	<p>If the HTTP request triggered the FortiWeb web caching feature, the message begins with [Replied by Cache].</p> <p>The HTTP/HTTPS request's:</p> <ul style="list-style-type: none"> • method • IP layer source and destination address and port numbers (IPv6 addresses are surrounded by square brackets to better demarcate the port number, e.g. [2001:470:19:ad7:6::230]:443) <p>such as:</p> <ul style="list-style-type: none"> • HTTP GET request from 10.0.2.5:8239 to 10.0.2.1:443 • HTTP POST request from 10.0.2.5:8100 to 10.0.2.1:80 <p>If the transaction used HTTPS, and there was an error when either decoding it or participating in the handshake, there may be an error message instead of the HTTP method, such as:</p> <p>HTTP request from 192.0.2.1:40170 to 10.0.2.1:443, <i>Ephemeral keys cannot be decrypted</i></p>
Source Country (srccountry)	The country that is the source of the traffic.
HTTP Content Routing (content_switch_name)	The name of the associated HTTP content routing policy.
Server Pool Name (server_pool_name)	The name of the server pool in the associated server policy.

Table 973:

Examples
<pre>date=2014-06-26 time=00:43:37 log_id=300000000 msg_id=000001351251 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT-8:00) Pacific Time(US&Canada)" type=traffic subtype="http" pri=notice proto=tcp service=http status=success reason=none policy=Auto-policy src=10.0.8.103 src_port=8142 dst=10.20.8.22 dst_port=80 http_request_time=0 http_response_time=0 http_request_bytes=444 http_response_bytes=401 http_method=get http_url="/" http_host="10.0.8.22" http_agent="Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; " http_retcode=200 msg="HTTP GET request from 10.0.8.103:8142 to 10.20.8.22:80" srccountry="Reserved" content_switch_name="testa" server_pool_name="Auto-ServerFarm"</pre>
<pre>date=2014-04-11 time=09:26:22 log_id=300000000 msg_id=000000000156 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=traffic subtype="http" pri=notification proto=tcp service=https status=success reason="none" policy="policy1" src=172.20.120.47 src_port=53817 dst=172.20.120.47 dst_port=80 http_request_time=18 http_response_time=1 http_request_bytes=464 http_response_bytes=3060 http_method=get http_url="/index" http_host="172.20.120.48" http_agent="Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0" http_retcode=200 msg="HTTPS GET request from 172.20.120.47:53817 to 172.20.120.47:80 " srccountry="United States" content_switch_name="testa" server_pool_name="Auto-ServerFarm"</pre>
<pre>date=2014-04-11 time=10:16:29 log_id=300000000 msg_id=000000000230 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00) Eastern Time(US & Canada)" type=traffic subtype="http" pri=notification proto=tcp service=http status=success reason="none" policy="policy1" src=172.20.120.46 src_port=49234 dst=172.20.120.48 dst_port=80 http_request_time=0 http_response_time=0 http_request_bytes=257 http_response_bytes=0 http_method=get http_url="/admin" http_host="172.20.120.48" http_agent="Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)" http_retcode=500 msg="HTTP POST request from 172.20.120.46:49234 to 172.20.120.48:80 " srccountry="United States" content_switch_name="testa" server_pool_name="Auto-ServerFarm"</pre>

